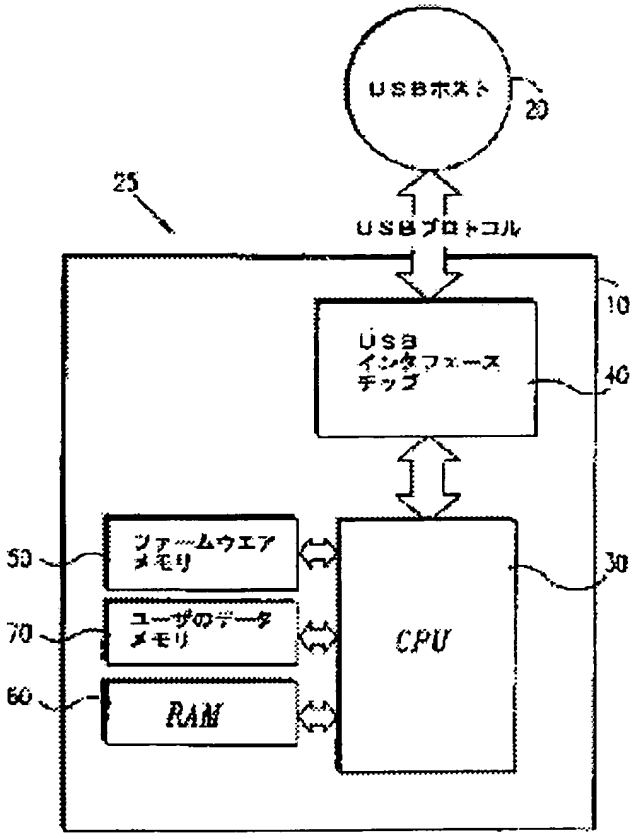
METHOD AND DEVICE FOR INTERACTION BETWEEN USER AND COMPUTER

Patent number: JP2000200248
Publication date: 2000-07-18
Inventor: MARGALIT YANKI; MARGALIT DANY; KASTERSHTIEN RAMI
Applicant: ALADDIN KNOWLEDGE SYSTEMS LTD
Classification:
- international: G06F15/00
- european:
Application number: JP19990302471 19991025
Priority number(s):

Also published as:
EP1001329 (A2)
EP1001329 (A3)

Abstract of **JP2000200248**

PROBLEM TO BE SOLVED: To flexibly improve a device which is freely connected by accepting an FCCS plug from a mobile user for a connection with a computer system and using information featuring the mobile user for its operation. SOLUTION: A USB interface chip 40 receives USB packets from a USB host 20 and analyzes and sends the data out to a microprocessor 30. The microprocessor 30 writes the data to a firmware memory 50, a RAM 60, or user's data memory 70 by using the protocol of respective memories or reads data out of it. In this case, the FCCS plug is used in relation to software having plug confirming capability as known before. The computer system received information featuring one mobile user in a group of mobile users and is frequently used to process the information, and the information featuring the mobile user is stored in the FCCS plug.



METHOD AND DEVICE FOR INTERACTION BETWEEN USER AND COMPUTER

Description of correspondent: **EP1001329**

FIELD OF THE INVENTION

[0001] The present invention relates to flexibly connectible computer apparatus and methods for using flexibly connectible hosts.

BACKGROUND OF THE INVENTION

[0002] The USB interface is described in specifications available over the Internet at www.usb.org.

[0003] Firewire technology, also termed "IEEE 1394 technology", is an alternative to USB which also provides flexible connectivity and is described in the IEEE 1394 standard.

[0004] USBHasp is an Aladdin software protection product, announced in October 1997, which includes a USB key. USBHasp does not control access of a user to a computer network but rather impedes interaction between software and a computer system by activating a copy of the software only if a USB key corresponding to that copy is plugged into the computer system.

[0005] Conventionally, the only devices which have interacted via USB have been computers, keyboard, monitor, printer, mouse, smart card readers, and biometric readers.

[0006] Conventional devices for providing computerized servicing to a mobile or stationary population of users typically include a smart card reader. The members of the mobile population bear smart cards which are used to interact with the computerized servicing device via the smart card reader.

[0007] A particular disadvantage of smart cards is that they require a smart card reader which is a relatively costly device. Computer hosts which are equipped with a smart card reader are a small subset of the universe of computer hosts because addition of a smart card reader makes the computer considerably more expensive.

[0008] German Patent document DE 19631050 describes an interface convener for a universal serial bus having a module with a processor that changes format and protocol into that of a different bus system.

[0009] Rainbow Technologies, Inc., in a news release dated 17 November 1998, announce USB software protection keys which can also be used as authentication or access control devices. A unique ID number if assigned to each USB key, enabling the key to replace or supplement personal passwords.The unique ID of the USB key makes it useful as a notebook computer security device providing theft deterrence. Other uses for the USB keys include Web access control, client token for Virtual Private Network access, replacement for password generator tokens and storage of credentials, certificates and licenses.

[0010] In a news release dated 19 January 1999, Rainbow Technologies, Inc. announce a new line of USB tokens for VPNs (virtual private networks) which provides end user client authentication to VPNs and enables operator access to secured network equipment. Features of these tokens include "Internet security small enough to fit on a key-ring" and "personalization for the end user". The tokens allow a user to keep personal information in his or her pocket rather than on a hard drive.

[0011] A new "unique per individual" model of its USB based tokens was announced by Rainbow Technologies Inc. on 15 March 1999.

[0012] The disclosures of all publications mentioned in the specification and of the publications cited therein are hereby incorporated by reference.

SUMMARY OF THE INVENTION

[0013] The present invention seeks to provide improved flexibly connectible apparatus and improved methods for using the same.

[0014] There is thus provided, in accordance with a preferred embodiment of the present invention, a user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method including storing information characterizing each mobile user on an FCCS plug to be borne by that mobile user and accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the information characterizing the mobile user to perform at least one computer operation.

[0015] Further in accordance with a preferred embodiment of the present invention, at least one computer operation comprises authentication.

[0016] Also provided, in accordance with another preferred embodiment of the present invention, is a an FCCS plug device to be borne by a mobile user, the FCCS plug device including a portable device which mates with a flexibly connectible computer system and comprises a memory and information characterizing the mobile user and stored in the memory accessibly to the flexibly connectible computer system.

[0017] Also provided, in accordance with another preferred embodiment of the present invention, is a population of FCCS plug devices to be borne by a corresponding population of mobile users, the population of FCCS plug devices including a multiplicity of portable devices each of which mates with a flexibly connectible computer system and comprises a memory and information characterizing each mobile user in the population of mobile users and stored, accessibly to the flexibly connectible computer system, in the memory of the FCCS plug device to be borne by the mobile user.

[0018] Additionally provided, in accordance with another preferred embodiment of the present invention, is an FCCS plug device including a mating element operative to mate with a flexibly connectible computer system and a memory connected adjacent the mating element, thereby to form a portable pocket-size plug, wherein the memory is accessible to the flexibly connectible computer system via the mating element.

[0019] Also provided, in accordance with another preferred embodiment of the present invention, is an FCCS plug device including a mating element operative to mate with a flexibly connectible computer system and a CPU connected adjacent the mating element thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via the mating element.

[0020] Further in accordance with a preferred embodiment of the present invention, the FCCS plug device also comprises a CPU connected adjacent the mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via the mating element.

[0021] Still further in accordance with a preferred embodiment of the present invention, at least one computer operation comprises digital signature verification and/or controlling access to computer networks.

[0022] Further in accordance with a preferred embodiment of the present invention, the information characterizing each mobile user comprises sensitive information not stored in the computer system, thereby to enhance confidentiality.

[0023] Also provided, in accordance with another preferred embodiment of the present invention, is a user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method including

storing confidential information not stored by the flexibly connectible computer systems on an FCCS plug to be borne by an individual user within the population of mobile users and
accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the confidential information to perform at least one computer operation, thereby to enhance confidentiality.

[0024] Preferably the apparatus also includes a microprocessor operative to receive the USB communications from the USB interface, to perform computations thereupon and to provide results of the computations to the data storage unit for storage and/or for encryption and/or for authentication and/or for access control.

[0025] The term "USB port" refers to a port for connecting peripherals to a computer which is built according to a USB standard as described in USB specifications available over the Internet at www.usb.org.

[0026] The term "USB plug" or "USB key" or "USB token" refers to a hardware device whose circuitry interfaces with a USB port to perform various functions.

[0027] The term "smart card" refers to a typically plastic card in which is embedded a chip which interacts with a reader, thereby allowing a mobile bearer of the smart card to interact with a machine in which is installed a smart card reader, typically with any of a network of machines of this type.

[0028] Also provided in accordance with a preferred embodiment of the present invention is an electronic token, which preferably mates with a flexible connection providing port such as the USB port of any computer system such as a PC, laptop, palmtop or peripheral. The electronic token preferably does not require any additional reading equipment. The token may authenticate information and/or store passwords or electronic certificates in a token which may be the size of a domestic house key.

[0029] Preferably, when the token is inserted into a flexible connection providing port, a highly secure "dual factor authentication" process (e.g. "what you have" plus "what you know") takes place in which (a) the electronic token is "read" by the host PCC or network and (b) the user types in his or her personal password for authorization.

[0030] Suitable applications for the electronic token include authentication for VPN, extranet and e-commerce.

[0031] The present invention also seeks to provide improved USB apparatus and improved methods for using the same.

[0032] There is thus provided, in accordance with another preferred embodiment of the present invention, USB key apparatus for interacting with a USB host via a USB port, the USB key apparatus including a portable device configured to fit the USB port, the portable device including a USB interface conveying USB communications to and from a USB host, a protocol translator operative to translate the USB communications from USB protocol, into smart card protocol such as an ISO7816 protocol, and from smart card protocol into USB protocol and a smart card chip operative to perform at least one smart card function such as authentication, encryption, access control and secure memory.

[0033] Also provided, in accordance with another preferred embodiment of the present invention, is USB key apparatus with data storage capabilities, the USB key apparatus including a portable device such as a PCB, configured to fit the USB port, the portable device including a USB interface conveying USB communications to and from a USB host and a data storage unit storing information derived from the USB communications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0034] The present invention will be understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified block diagram of a USB plug device including a CPU and a non-ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention;
Fig. 2 is a simplified block diagram of a USB plug device including a CPU and a ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention;
Fig. 3 is an exploded front view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB plug device of Fig. 1;
Fig. 4 is an exploded view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB plug device of Fig. 2; and
Figs. 5A - 5B pictorially illustrate a user-computer interaction method provided in accordance with a preferred embodiment of the present invention for use by a population of flexibly connectible computer systems and a population of mobile users.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0035] Reference is now made to Fig. 1 which is a simplified block diagram of a flexibly connectible USB plug device including a CPU and a non-ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention.

[0036] A particular feature of the USB plug device of Fig. 1 is that it has data storage capabilities and is thus analogous to a memory smart card.

[0037] The USB plug device 10 comprises a PCB 25 which includes a microprocessor or CPU 30 such as a Motorola 6805, Cypress chip or Intel 8051; a USB interface device 40; firmware memory 50 serving the firmware of the microprocessor 30; RAM memory 60 of size sufficient to enable contemplated computations on the part of the microprocessor 30; and user data memory 70 which stores a user's data. Some or all of the USB interface device 40, firmware memory 50 and RAM memory 60 may be within the CPU 30.

[0038] The USB interface device 40 and/or the firmware memory 50 may be integrated inside the microprocessor 30.

[0039] The firmware memory may be any suitable type of memory such as but not limited to ROM, EPROM, EEPROM or FLASH.

[0040] The user data memory 70 typically does not include ISO7816-3 memory and may, for example, comprise any of the following types of memory: I<2>C, XI<2>C, 2/3 wire bus, FLASH.

[0041] As shown, the USB plug device 10 is configured to interact with any USB host 20 such as but not limited to a personal computer or Macintosh having a USB port. Key-host interaction is governed by a USB protocol such as the USB protocol described in the USB specifications available over the Internet at www.usb.org. USB packets pass between the USB host 20 and the USB interface chip 40. Each packet typically includes the following components:

a. USB header;
b. Data to be stored/read on the user's data memory 70, plus additional information required by protocols of the memory chip 70, such as but not limited to the address to store/read the data, the length of data to store/read, and CRC checksum information.
c. USB footer.

[0042] The flow of data typically comprises the following flow:

[0043] The USB interface chip 40 receives USB packets from the USB host 20, parses the data, and feeds the parsed data to the microprocessor 30. The microprocessor 30 writes the data to, or reads the data from, the firmware memory 50, the RAM 60 or the user's data memory 70, using each memory's protocol.

[0044] In read operation, the microprocessor 30 passes the data to the USB interface chip 40 which wraps the data in USB packet format and passes it to the host 20.

[0045] Fig. 2 is a simplified block diagram of a USB plug device, constructed and operative in accordance with a preferred embodiment of the present invention, which is a one-piece smart card reader and smart card chip preferably providing both secured storage and cryptographic capabilities. The USB plug device of Fig. 2 includes both a CPU and a smart card chip (ICC) memory 170, typically a ISO7816 (T = 0/1) protocol-based chip communicating with the CPU 130 using an ISO7816-3 protocol. The apparatus of Fig. 2 is similar to the apparatus of Fig. 1 except that no separate user's data memory 70 is provided. The size of the RAM 160 is typically at least 262 bytes in order to support the ISO 7816_3 T=0 or T=1 protocols.

[0046] Each packet typically includes the following components:

a. USB header;
b. ISO7816-3 T=0/1 protocol packet;
c. USB footer.

[0047] The flow of data in the apparatus of Fig. 2 typically comprises the following flow:

[0048] The USB interface chip 140 gets USB packets from the USB host 120. The USB interface chip 140 parses the data and passes it to the microprocessor 130. The data, which typically comprises a ISO7816-3 T=0/1 formatted packet, is passed by the microprocessor to the smart-card 170 in a ISO7816-3 protocol. The microprocessor 130 gets the response from the smart card 160 and passes the data to the USB interface chip 140. The USB interface chip 140 wraps the data in USB packet format and passes it to the host 120.

[0049] A particular advantage of the embodiment of Fig. 2 is that smart card functionality is provided but there is no need for a dedicated reader because the plug 110 is connected directly to a USB socket in the host 120.

[0050] The invention shown and described herein is particularly useful for computerized systems serving organizations which process sensitive information such as banks, insurance companies, accountants and other commercial organizations, and professional organizations such as medical or legal organizations.

[0051] Conventional computer systems include a computer (comprising a motherboard) and at least one peripherals. The computer has a number of different ports which respectively mate with the ports of the various peripherals. Each port typically can mate with only certain peripherals and not with other peripherals. For example, the keyboard cannot be connected to the computer via the computer's printer port.

[0052] In state of the art computer systems, also termed herein "flexibly connectible computer systems", the computer and the peripherals each include at least one identical ports having mating ports on any other computer and any other peripheral such that any peripheral can be selectably connected to any computer or to any other peripheral. Also, a peripheral may be connected to the computer not directly as in conventional systems but rather via another peripheral. There is generally always a port available on one or more connected peripherals in an existing computer system such that another peripheral can generally always be connected to an existing computer system.

[0053] One example of a flexibly connectable computer system is a USB (universal standard bus) system in which the computer and each peripheral includes a USB port. Another example of a flexibly connectable computer system is the recently contemplated Firewire system.

[0054] A "USB plug" is a portable device which mates with a USB system and, as opposed to peripherals which contain mechanical elements, typically comprises only memory and/or CPU and therefore is typically pocket-size. More generally, a USB plug is an example of a plug which can be plugged into a flexibly connectible computer system (FCCS).

[0055] The term "FCCS plug" is used herein to refer to a portable device which mates with a flexibly connectible computer system and, as opposed to peripherals which contain mechanical elements, typically comprises only

memory and/or CPU and therefore is typically pocket-size. It is appreciated that because each peripheral connected onto a flexibly connectible computer system typically has at least one port, therefore, a flexibly connectible computer system of any configuration typically has at least one vacant port available to interact with an FCCS plug. USB tokens and Rainbow tokens are both examples of FCCS plugs.

[0056] Typically, each of the plurality of computer system units (computer and one or more peripherals) forming a computer system has at least two identical female sockets and these are interconnected by means of male-male cables. In this embodiment, the FCCS plug may comprise a male socket. However, it is appreciated that any suitable mating scheme may be employed to mate the computer system units and the the FCCS plug of the present invention.

[0057] A known use for FCCS plugs is use in conjunction with software having plug-recognizing capability. Aladdin and Rainbow both market software which is operative only if the host computer system in which a particular software copy resides has plugged into it an FCCS plug which is recognized by the software copy. The Aladdin and Rainbow plugs are not used for authentication.

[0058] Computer systems are often used to receive information characterizing a mobile user, who is one of a population of mobile users, and to process this information. Such information may comprise user identity authentication information, banking information, access rights information, etc. Conventionally, this information is stored on a smart card which is borne by the user and is presented to the computer system by him. However this requires the computer system to be equipped with a smart card reader, a special piece of equipment dedicated to reading the smart card.

[0059] According to a preferred embodiment of the present invention, information characterizing a mobile user is stored on an FCCS plug. Particular advantages of this embodiment of the present invention is that the information is easily borne by the user, on a pocketsize substrate, that any flexibly connectible computer system of any configuration is typically capable of interacting with the user via the FCCS plug, and that no dedicated equipment is required by the computer in order to carry out the interaction:

[0060] Reference is now made to Fig. 3 which is an exploded front view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB key device of Fig. 1. As shown, the FCCS plug of Fig. 3 comprises a housing typically formed of two snap-together planar cover elements 200 and 210, between which reside a USB connector 220 and the PCB 25 of Fig. 1. The USB connector 220 may, for example comprise a USB PLUG SMT &lang&ACN-0213&rang& device marketed by Aska Technologies Inc., No. 15, Alley 22, Lane 266, Fu Teh, 1st Rd., Hsl Chih, Talpei Shien, Taiwan. The PCB 25 bears the elements 30, 40, 50, 60 and 70 of Fig. 1. Firmware managing the memory 240 may reside on the USB interface controller 230.

[0061] Reference is additionally made to Fig. 4 which is an exploded view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB key device of Fig. 2. As shown, the FCCS plug of Fig. 4 comprises a housing typically formed of two snap-together planar cover elements 200 and 210, between which reside the USB connector 220 and a PCB 125. The PCB 125 bears the elements 130, 140, 150, 160 and 170 of Fig. 2. Firmware managing the smart card chip 250 may reside on the USB interface controller 230.

[0062] Smart card functionalities which are preferably provided by the FCCS plug of the present invention include:

1. Controlling access to computer networks: Smart card or plug has ID information, network authenticates and allows access on that basis. Authentication may be based upon "what you have", "what you are" e.g. biometric information and "what you know" (e.g. password).
2. Digital signatures or certificates for verifying or authenticating the identity of the sender of a document.
3. Storage of confidential information e.g. medical information. A smart card or plug may store confidential information and interact with a network which does not store the confidential information.

[0063] Figs. 5A - 5B pictorially illustrate a user-computer interaction method provided in accordance with a preferred embodiment of the present invention for use by a population of flexibly connectible computer systems 300 and a population of mobile users. Information characterizing each mobile user, e.g. name and ID, is loaded into the

memory of an FCCS plug 310 to be borne by that mobile user, typically via a USB interface controller such as unit 230 of Fig. 3.

[0064] The plug can then be connected to one of the flexibly connectible computer systems and the information characterizing the mobile user employed to perform at least one computer operation typically comprising a conventional smart card functionality such as authentication.

[0065] Features of a preferred embodiment of the present invention are now described:

a. The need for enhanced user authentication

Authentication is the basis for any information security system. The ability to authenticate local and remote users is a critical issue for any LAN/Intranet, multi-user environment

b. The need for encryption and confidentiality

Content encryption & confidentiality becomes an important issue for both the corporation and the individual users

c. The need for password and Sign-On security

Password security and user password management are key issues for network corporate users. Passwords represent the single most important security concern in any computing environment

[0069] There is a need today for hardware-based PC security tokens

Sign-On-Key (SOK) is a hardware-based token that seamlessly integrates with Operating Systems & Applications to provide:

- a user authentication key
- a basis for encryption system
- better Sign-On security and enhanced user password management
- Software Security

Authentication - 3 Basic Elements

Something you know –> Password

Something you have --> Sign-On-Key
Something you are --> e.g., Bio-metrics
Assumption: Two out of the above three provide "good-enough" security.

Encryption

The need to encrypt data, files, disks and information flow is evident.
An hardware-based token with cryptographic abilities can enhance security and ease-of use.

Sign-On - Where are Passwords used?

Log on to your O/S
Log on to your Network (Local, Remote)
Log on to the Internet/ISP
Log on to protected Web pages
Log on to Group Ware/Communications applications
Log on to other sensitive password-protected applications
MS Office & other protected files
PC Boot protection (Bios Password)

Sign-On - Major Security Risks

The Sign-On Process

[0073] The Sign-On-Key is a security hardware token, linked by the user to the required applications. Once installed the -Sign-On-Key becomes a part of the log-on process. Sign-On-Key provides the user with many security and other functional benefits.

What Can Sign-On-Key Do For a User?

Sign-On Security

- Enhance security & authentication. The Sign-On-Key is required in addition to the user password

Sign-On Simplicity

- Simplify log-on process and eliminate the need for a password. The Sign-On-Key replaces the password

Password Automatic Re-verification

- Check for Sign-On-Key periodically

Single-Sign-On

- One Sign-On-Key replaces several passwords for several applications

Mobility & Remote Computing

- Sign-On-Key identifies remote users
- Sign-On-Key can be used as a data secure container
- Theft deterrent of mobile PCs

General Purpose Security Token

- File & data Encryption
- Authentication
- Certificate Key Holder

Sign-On-Key Various Options

Several hardware devices may operate as Sign-On-Keys:

- Sign-On-Key USB - A small key that connects to the new standard USB port. USB ports are becoming the new connectivity standard for PCs and Macintosh
- Sign-On-Key SC - A smart card based Sign-On-Key. Can be used with any standard smart card drive

Sign-On-Key USPs & Advantages

Simple, intuitive, easy to use, attractive token
The key IS the token IS the connector
Low cost
High security
High functionality

- Memory inside token
- Processing power
- Automatic Password Re-verification
- Multi token connectivity

The Agents' solution

Sign-On-Key Architecture

Full Blown System.

Sign On Agents

The Sign-On-Agent is a software interface between the Sign-On-Key and the application.
The Sign-On-Boot is a special interface for the PC boot password.
Agents may be provided for:

- OS/Net Ware - e.g., Windows NT, 95/98, 3x, Novell, Unix
- Group Ware/Mail - e.g, Lotus Notes, Outlook, Eudora,
- Enterprise Applications - e.g., SAP, Baan, MK, Oracle, Magic
- Web Browsers - e.g., Explorer, Navigator

The Most Trivial Agent - Windows NT

The most trivial Agent will replace the Windows Login session
By doing so Users may gain

- Windows Login Extra security
- Windows Login simplification (Sign-On-Key replaces password)

Sign-On-Key Web Browsers' Agent/System

Sign-On-Key can be used as an authentication token to monitor access to secured web pages
Web content providers need to authenticate, manage and provide access to their customers

Sign-On-Key API (SDK)

Sign-On-Key API is the interface level between the Sign-On-Key and 3rd parties' applications.
This API may be published and opened for usage by certification providers, security companies and SSO companies.

The Sign-On-Key API will also provide encryption & protected memory storage services
Sign-On-Key API may be PKCS #11 based/compatible

The Sign-On Process (No CA)

Installation

- User installs Agents for required applications
- User defines Sign-On Parameters for each application
- User stores Sign-On information in Sign-On-Key

Sign-On

- Application is started
- Application reaches its Sign-On dialog
- Application communicates with the Sign-On-Key
- Sign-On permission is granted based on Sign-On-Key

Sign-On-Key As a Secure Container

In addition to unique Key ID, Sign-On-Key will contain personal protected memory area
This memory area can be used for storing sensitive information and Certificates
Applications' ID keys like Lotus Notes ID file or PGP keys can be stored in this memory
Doing so - Sign-On-Key can be used to increase mobile computing security. Files IDs are stored in Sign-On-Key instead of disk

Sign-On-Key An Encryption Engine & Sign-On-Key Crypt

Sign-On-Key can be used as an encrypting device
An encryption API may be provided, e.g., a 100% smart card compatible Sign-On-Key implementation
Sign-On-Key Crypt is a Data/File/Hard disk encryption utility based on Sign-On-Key.

Sign-On-Key Certification Toolkit

SOK may use PKCS #11 and X509 and store certificates and/or digital IDs.

Sign-On-Key comprises:

Sign-On-Key USB Token
HASP
Hardlock
Initial Sign-On-Key functionality(Unique ID, personal protected memory)
Sign-On-Key USB extension cable
Sign-On-Key Smart Card Token
Sign-On-Key API (PKCS #11 compliant)
Entrust compatibility/link
Windows NT Agent
Navigator and/or Explorer Agent (S/Mime)
Key Plus Crypt (Beta release)
Secure Screen Saver
Initial marketing package
USB proliferation & Windows 98/NT availability are key issues
In the US, Germany & Israel all new PCs shipped are USB equipped.
Section in Early Development stage.
Security Dynamics, ActivCard & Vasco control the market with 1st generation time-based, one-time password or challenge-based tokens
security vendors will look to expand their market share with second generation integrated smart card offerings which will support cryptography, digital signature storage and processing activity

USB: The Better Connection

Almost unlimited port expansion
No add-in cards for new peripherals

- no setting of IRQs, DMAs, etc.

One connection type (plug and port)

- variety of peripherals
- no more guesswork
- simple setup, just plug in and go

USB: The Better Connection

Addresses need for speed, multimedia

- 12 Mb/s, Asynch (bulk) & Isoch (real time) data

- stereo-quality digital audio
- high frame-rate video (with compression)
- high latency applications (force-feedback)

No power bricks with many new peripherals

- USB supplies up to 500mA

PC User experience is vastly improved

- Fewer returns and increased sales potential

[0088] It is appreciated that USB is only one example of a flexible connectivity standard and the present invention is not intended to be limited to USB.

[0089] It is appreciated that the software components of the present invention may, if desired, be implemented in ROM (read-only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques.

[0090] It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

[0091] It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention is defined only by the claims that follow:

[0092] Where technical features mentioned in any claim are followed by reference signs, those reference signs have been included just for the sole purpose of increasing intelligibility of the claims and accordingly, such reference signs do not have any limiting effect on the scope of each element identified by way of example by such reference signs.

METHOD AND DEVICE FOR INTERACTION BETWEEN USER AND COMPUTER

Claims of correspondent: **EP1001329**

1. A user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method comprising:

storing information characterizing each mobile user on an FCCS plug to be borne by that mobile user; and accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the information characterizing the mobile user to perform at least one computer operation.

2. A method according to claim 1 wherein said at least one computer operation comprises authentication.

3. An FCCS plug device to be borne by a mobile user, the FCCS plug device comprising:

a portable device which mates with a flexibly connectible computer system and comprises a memory; and information characterizing the mobile user and stored in said memory accessibly to the flexibly connectible computer system.

4. A population of FCCS plug devices to be borne by a corresponding population of mobile users, the population of FCCS plug devices comprising:

a multiplicity of portable devices each of which mates with a flexibly connectible computer system and comprises a memory; and
information characterizing each mobile user in the population of mobile users and stored, accessibly to the flexibly connectible computer system, in the memory of the FCCS plug device to be borne by said mobile user.

5. An FCCS plug device comprising:

a mating element operative to mate with a flexibly connectible computer system; and
a memory connected adjacent said mating element, thereby to form a portable pocket-size plug, wherein the memory is accessible to the flexibly connectible computer system via said mating element.

6. An FCCS plug device comprising:

a mating element operative to mate with a flexibly connectible computer system; and
a CPU connected adjacent said mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via said mating element.

7. An FCCS plug device according to claim 5 and also comprising a CPU connected adjacent said mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via said mating element.

8. A method according to claim 1 wherein said at least one computer operation comprises digital signature verification.

9. A method according to claim 2 wherein said at least one computer operation comprises controlling access to computer networks.

10. A method according to claim 1 wherein said information characterizing each mobile user comprises sensitive information not stored in said computer system, thereby to enhance confidentiality.

11. A user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method comprising:

storing confidential information not stored by the flexibly connectible computer systems on an FCCS plug to be borne by an individual user within said population of mobile users; and
accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the confidential information to perform at least one computer operation, thereby to enhance confidentiality.

12. USB key apparatus for interacting with a USB host via a USB port, the USB key apparatus comprising:

a portable device configured to fit the USB port, the portable device comprising:

a USB interface conveying USB communications to and from a USB host;
a protocol translator operative to translate the USB communications from USB protocol into smart card protocol and from smart card protocol into USB protocol; and
a smart card chip operative to perform at least one smart card function.

13. USB key apparatus according to claim 12 wherein the smart card protocol comprises an ISO7816 protocol.

14. USB key apparatus with data storage capabilities, the USB key apparatus comprising:

a portable device configured to fit a USB port, the portable device comprising:

a USB interface conveying USB communications to and from a USB host; and
a data storage unit storing information derived from the USB communications.

15. Apparatus according to claim 12 wherein the smart card function comprises at least one function selected from the group consisting of secured memory, authentication, encryption and access control.

16. Apparatus according to claim 14 and also comprising a microprocessor operative to receive said USB communications from the USB interface, to perform computations thereupon and to provide results of the computations to the data storage unit for storage.

17. A method for interacting with a USB host via a USB port, the method comprising:

configuring a portable device to fit the USB port;
conveying USB communications to and from a USB host;
translating the USB communications from USB protocol into smart card protocol and from smart card protocol into USB protocol; and
providing a smart card chip operative to perform at least one smart card function.

18. A method according to claim 17 wherein the smart card protocol comprises an ISO7816 protocol.

19. A data storage method comprising:

configuring a portable device to fit a USB port;

conveying USB communications to and from a USB host; and
storing information derived from the USB communications.

20. A method according to claim 17 wherein the smart card function comprises at least one function selected from the group consisting of secured memory, authentication, encryption and access control.

21. A method according to claim 19 and also comprising employing a microprocessor to receive said USB communications from the USB interface, to perform computations thereupon and to provide results of the computations to the data storage unit for storage.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－200248
(P2000－200248A)
(43)公開日　平成12年７月18日(2000.7.18)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ

審査請求　未請求　請求項の数21　ＯＬ　外国語出願　（全 38 頁）

(21)出願番号　特願平11－302471

(22)出願日　平成11年10月25日(1999.10.25)

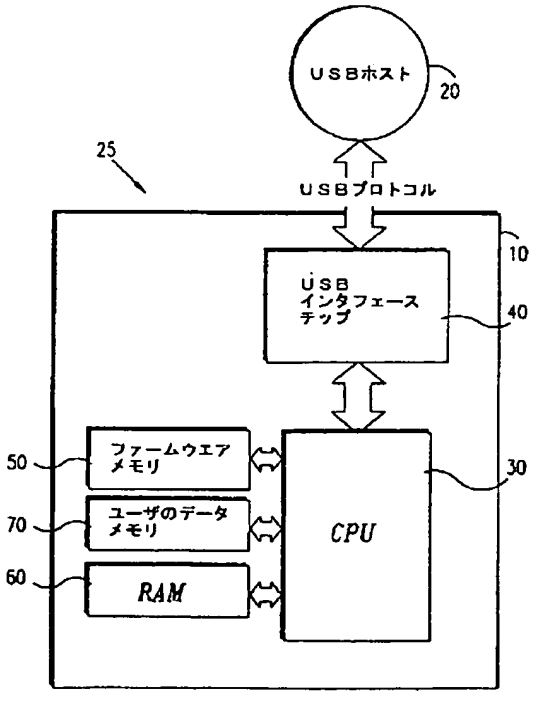
(31)優先権主張番号　０９／１８９９６０
(32)優先日　平成10年11月10日(1998.11.10)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／４１２２９２
(32)優先日　平成11年10月５日(1999.10.5)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　599150171
アラディン・ノリッジ・システムズ・リミテッド
イスラエル国テル・アビブ　67211，ベイト・オベド・ストリート　15
(72)発明者　ヤンキ・マルガリト
イスラエル国ラマト・ガン　52223，キリアティ・ストリート　7
(72)発明者　ダニ・マルガリト
イスラエル国ラマト・ガン　52223，キリアティ・ストリート　10
(74)代理人　100089705
弁理士　社本　一夫　（外４名）

最終頁に続く

(54)【発明の名称】　ユーザとコンピュータ間の対話方法及び装置

(57)【要約】
【課題】改良されたフレキシブルに接続自在な装置と、それを用いる改良された、ユーザとコンピュータ間の対話方法を提供する。
【解決手段】一群のフレキシブルに接続自在のコンピュータ・システムと、一群の移動ユーザとにより使用されるユーザとコンピュータ間の対話方法であって、各移動ユーザにより保有されるＦＣＣＳプラグにその移動ユーザを特徴づける情報を記憶するステップと、移動ユーザからＦＣＣＳプラグを受け、フレキシブルに接続自在のコンピュータ・システムの一つへの接続に供するステップと、更に移動ユーザを特徴づける情報を用いて少なくとも一つのコンピュータ動作を行うステップとで構成される。



【特許請求の範囲】
【請求項１】 一群のフレキシブルに接続自在なコンピュータ・システムおよび一群の移動ユーザにより使用されるユーザとコンピュータ間の対話方法であって、
この移動ユーザにより保有されるＦＣＣＳプラグに各移動ユーザを特徴づける情報を記憶するステップと、
フレキシブルに接続自在なコンピュータ・システムの一つに接続するために移動ユーザからＦＣＣＳプラグを受容し、且つ少なくとも一つのコンピュータ動作を行うために移動ユーザを特徴づける情報を用いるステップと、を含むユーザとコンピュータ間の対話方法。
【請求項２】 前記少なくとも一つのコンピュータ動作は、認証を含む請求項１に記載の方法。
【請求項３】移動ユーザにより保有されるＦＣＣＳプラグ装置であって、
フレキシブルに接続自在なコンピュータ・システムと連接すると共に、メモリを含むポータブル装置と、
移動ユーザを特徴づけ、且つフレキシブルに接続自在なコンピュータ・システムにアクセス自在に前記メモリに記憶される情報と、を含むＦＣＣＳプラグ装置。
【請求項４】対応する一群の移動ユーザにより保有される一群のＦＣＣＳプラグ装置であって、
フレキシブルに接続自在なコンピュータ・システムと連接し、且つメモリを含む多数のポータブル装置と、
一群の移動ユーザにおける各移動ユーザを特徴づけ、且つフレキシブルに接続自在なコンピュータ・システムにアクセス自在に、前記移動ユーザにより保有されるＦＣＣＳプラグのメモリに記憶される情報と、を含むＦＣＣＳプラグ装置。
【請求項５】 フレキシブルに接続自在なコンピュータ・システムと連接するように動作する連接素子と、
前記連接素子に隣接して接続され、これによりポケットサイズのポータブル・プラグを形成するメモリと、を含み、
前記メモリは、前記連接素子を介して、フレキシブルに接続自在なコンピュータ・システムにアクセス自在である、ＦＣＣＳプラグ装置。
【請求項６】 フレキシブルに接続自在なコンピュータ・システムと連接するように動作する連接素子と、
前記連接素子と隣接して接続され、これによりポケットサイズのポータブル・プラグを形成するＣＰＵと、を含み、
前記ＣＰＵは、前記連接素子を介して、フレキシブルに接続自在なコンピュータ・システムへのデータ接続を有する、ＦＣＣＳプラグ装置。
【請求項７】 前記連接素子に隣接して接続され、これによりポケットサイズのポータブル・プラグを形成するＣＰＵを更に含み、
前記ＣＰＵは、前記連接素子を介して、フレキシブルに接続自在のコンピュータ・システムへのデータ接続を有する、請求項５に記載のＦＣＣＳプラグ装置。
【請求項８】 前記少なくとも一つのコンピュータ動作は、デイジタル署名検証を含む請求項１に記載の方法。
【請求項９】 前記少なくとも一つのコンピュータ動作は、コンピュータ・ネットワークへのアクセスを制御することを含む請求項２に記載の方法。
【請求項１０】各移動ユーザを特徴づける前記情報は、前記コンピュータ・システムに記憶されない機密情報を含み、これにより機密性を増強させる請求項１に記載の方法。
【請求項１１】一群のフレキシブルに接続自在のコンピュータ・システムと一群の移動ユーザにより使用されるユーザとコンピュータ間の対話方法であって、
前記一群の移動ユーザ内の個別ユーザにより保有されるＦＣＣＳプラグにフレキシブルに接続自在のコンピュータ・システムにより記憶されない機密情報を記憶するステップと、
フレキシブルに接続自在のコンピュータ・システムの一つへの接続のため移動ユーザからＦＣＣＳプラグを受容し、機密情報を用いて少なくとも一つのコンピュータ動作を行い、これにより機密性を向上させるステップと、を含むユーザとコンピュータ間の対話方法。
【請求項１２】ＵＳＢポートを介してＵＳＢホストと対話するための、ＵＳＢポートに適合するように形成されたポータブル装置を含むＵＳＢキー装置であって、
前記ポータブル装置は、
ＵＳＢホストへ、およびＵＳＢホストから、ＵＳＢ通信を搬送するＵＳＢインタフェースと、
ＵＳＢプロトコルからスマート・カード・プロトコルへ、およびスマート・カード・プロトコルからＵＳＢプロトコルへ、ＵＳＢ通信を翻訳するように動作するプロトコル・トランスレータと、
少なくとも一つのスマート・カード機能を行うように動作するスマート・カードチ・チップと、を含むＵＳＢキー装置。
【請求項１３】前記スマート・カード・プロトコルは、ＩＳＯ７８１６プロトコルを含む請求項１２に記載のＵＳＢキー装置。
【請求項１４】データ記憶能力を有する、ＵＳＢポートに適合するように形成されたポータブル装置を含むＵＳＢキー装置であって、
前記ポータブル装置は、
ＵＳＢホストへ、およびＵＳＢホストから、ＵＳＢ通信を搬送するＵＳＢインタフェースと、
ＵＳＢ通信から得られた情報を記憶するデータ記憶ユニットと、を含むＵＳＢキー装置。
【請求項１５】前記スマート・カード機能は、確保されたメモリ、認証、暗号化、およびアクセス制御からなる群から選択された少なくとも一つの機能を含む請求項１２に記載の装置。

【請求項16】前記USB通信をUSBインタフェースから受信し、それに対する計算を行い、且つ計算の結果を前記データ記憶ユニットに与えて記憶するように動作するマイクロプロセッサを更に含む、請求項14に記載の装置。

【請求項17】USBポートを介してUSBホストと対話する方法であって、

USBポートに適合するようにポータブル装置を形成するステップと、

USBホストへ、およびUSBホストから、USB通信を搬送するステップと、

USBプロトコルからスマート・カード・プロトコルに、且つスマート・カード・プロトコルからUSNBプロトコルに、USB通信を翻訳するステップと、

少なくとも一つのスマート・カード機能を行うように機能するスマート・カード・チップを与えるステップと、を含むUSBホストと対話する方法。

【請求項18】前記スマート・カード・プロトコルは、ISO7816プロトコルを含む請求項17に記載の方法。

【請求項19】USBポートに適合するようにポータブル装置を形成するステップと、

USBホストへ、およびUSBホストから、USB通信を搬送するステップと、

USB通信から得られた情報を記憶するステップと、を含むデータ記憶方法。

【請求項20】前記スマート・カード機能は、確保されたメモリ、証明、暗号化、およびアクセス制御からなる群から選択された少なくとも一つの機能を含む請求項17に記載の方法。

【請求項21】マイクロプロセッサを用いて、前記USB通信をUSBインタフェースから受信し、それに対して計算を行い、且つ計算の結果を前記データ記憶ユニットへ与えて記憶するステップを更に含む請求項19に記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、フレキシブルに接続自在なコンピュータ装置、およびフレキシブルに接続自在なホストを用いる方法に関する。

【0002】

【発明の背景】USBインタフェースは、www.usb.orgにおけるインターネット上で得られる仕様書に記載されている。

【0003】フアイヤワイヤ技術は、「IEEE1394技術」とも呼ばれ、またフレキシブルな結合性を与え且つIEEE1394標準に記載されたUSBに代わるものである。

【0004】USBHaspは、USBキーを含む、1997年10月に発表されたAladdinのソフトウエア保護製品である。USBHaspは、ユーザのコンピュータ・ネットワークへのアクセスを制御するのではなく、むしろソフトウエアのコピーに対応するUSBキーがコンピュータ・システムに差し込まれたときにのみ、このコピーを活性化することによりソフトウエアとコンピュータ・システム間の対話を妨害するものである。

【0005】従来、USBを介して対話する装置は、コンピュータ、キーボード、モニタ、プリンタ、マウス、スマート・カード・リーダ、バイオメトリック・リーダに過ぎない。

【0006】一群の移動または静止ユーザに対してコンピュータ化されたサービスを与える従来の装置は、通常スマート・カード・リーダを含む。一群の移動メンバーは、スマート・カード・リーダを介してコンピュータ化されたサービス装置と対話するために用いられるスマート・カードを保有する。

【0007】スマート・カードの特定の欠点は、比較的高価な装置であるスマート・カード・リーダを必要とするという点にある。スマート・カード・リーダを備えるコンピュータ・ホストは、スマート・カード・リーダを付加するとコンピュータがかなり高価になるということから、全世界のコンピュータ・ホストのうちの小さなサブセットである。

【0008】ドイツ特許公報DE19631050号は、フォーマットおよびプロトコルを異なるバス・システムのそれに変えるプロセッサを備えたモジュールを有する万能直列バスに対するインタフェース・コンバータを示している。

【0009】1998年11月17日付けのニュース・リリースにおいて、RainbowTechnologies社は、認証またはアクセス制御装置としても使用できるUSBソフトウエア保護キーを発表している。独自のIDナンバーは、各USBキーに割り当てられたとき、キーによって個人のパスワードを置き換え、または補足することを可能にする。USBキーの独自のIDは、このキーを、盗難防止を与えるノートブック・コンピュータ・セキュリテー装置として有用にする。USBキーの他の使用法には、ウエブ・アクセス制御や、仮想プライベート・ネットワーク・アクセスに対するクライアント・トークン、パスワード発生器トークンの置き換え、信任、証明およびライセンスの記憶、などがある。

【0010】1999年1月19日付けのニュース・リリースにおいて、RainbowsTechnologies社は、エンド・ユーザ・クライアントの認証をVPN（仮想プライベート・ネットワーク）に与え、確保されたネットワーク装置へのオペレータ・アクセスを可能にするVPNに対する新しいラインのUSBトークンを発表している。これらのトークンの特徴には、「キー・リングに適合するのに充分小さなインターネット・セ

キュリテー」および「エンド・ユーザに対する個性化」というものが含まれる。トークンによって、ユーザは個人情報をハード・ドライブよりむしろ彼または彼女のポケットに保持することができる。

【００１１】ＵＳＢに基づくトークンの新らしい「個人毎に独自の」モデルが、１９９９年３月１５日にＲａｉｎｂｏｗｓ　Ｔｅｃｈｎｏｌｏｇｉｅｓ社により発表された。本明細書で示された全ての出版物およびそれにサイトされた出版物の開示がここで引用により取り込まれる。

【００１２】

【発明の要約】本発明は、改良されたフレキシブルに接続自在な装置およびこの装置を用いるための改良された方法を提供する。

【００１３】本発明の好適な実施例に従って、フレキシブルに接続自在な一群のコンピュータ・システムおよび一群の移動ユーザにより使用されるユーザとコンピュータ間の対話方法であって、移動ユーザにより保有されるＦＣＣＳプラグに各移動ユーザを特徴づける情報を記憶し、フレキシブルに接続自在なコンピュータ・システムの一つへの接続のために移動ユーザからＦＣＣＳプラグを受容し、更に移動ユーザを特徴づける情報を用いて少なくとも一つのコンピュータ動作を行うステップを含む方法である。

【００１４】更に、本発明の好適な実施例により、少なくとも一つのコンピュータ動作は認証を含む。更に、本発明の他の好適な実施例によれば、移動ユーザにより保有されるＦＣＣＳ装置であって、フレキシブルに接続自在なコンピュータ・システムと連接すると共にフレキシブルに接続自在なコンピュータ・システムにアクセス自在にメモリに記憶されるポータブル装置を備えるＦＣＣＳプラグ装置が提供される。

【００１５】更に、本発明の他の好適な実施例によれば、対応する一群の移動ユーザにより保有される一群のＦＣＣＳプラグ装置であって、この一群のＦＣＣＳプラグ装置が多数のポータブル装置を含み、これらポータブル装置の各々が、フレキシブルに接続自在なコンピュータ・システムと連接し、且つメモリと、一群の移動ユーザにおいて各移動ユーザを特徴づけると共に移動ユーザにより保有されるＦＣＣＳプラグ装置のメモリにおいてフレキシブルに接続自在なコンピュータ・システムにアクセス自在に記憶される情報とを含む、一群のＦＣＣＳプラグ装置が提供される。

【００１６】更に、本発明の他の好適な実施例によれば、フレキシブルに接続自在なコンピュータ・システムと連接するように動作する連接素子と、この連接素子に隣接して接続され、それによりポケットサイズのポータブル・プラグを形成し、連接素子を介して、フレキシブルに接続自在なコンピュータ・システムにアクセス自在なメモリとを備えたＦＣＣＳプラグ装置が提供される。

【００１７】更に、本発明の他の実施例によれば、ＦＣＣＳプラグ装置であって、フレキシブルに接続自在なコンピュータ・システムと連接するように動作する連接素子と、この連接素子に隣接して接続され、これによりポケットサイズのポータブル・プラグを形成し、連接素子を介して、フレキシブルに接続自在なコンピュータ・システムに対するデータ接続を有するＣＰＵとを備えたＦＣＣＳプラグ装置が提供される。

【００１８】更に、本発明の好適な実施例によれば、ＦＣＣＳプラグ装置は、連接素子に隣接して接続され、これによりポケットサイズのポータブル・プラグを形成し、連接素子を介して、フレキシブルに接続自在なコンピュータ・システムに対してデータ接続を持つＣＰＵを含む。

【００１９】更に、本発明の好適な実施例によれば、少なくとも一つのコンピュータ動作はデジタル署名の検証および／またはコンピュータ・ネットワークへのアクセスを制御することを含む。

【００２０】更に、本発明の好適な実施例によれば、各移動ユーザを特徴づける情報は、コンピュータ・システムに記憶されない機密情報からなり、これにより機密性を増強させる。

【００２１】更に、本発明の他の好適な実施例によれば、フレキシブルに接続自在な一群のコンピュータ・システムおよび一群の移動ユーザによる使用に供するユーザとコンピュータ間の対話方法であって、一群の移動ユーザ内で個別ユーザにより保有されるＦＣＣＳプラグにフレキシブルに接続自在なコンピュータ・システムにより記憶されない機密情報を記憶し、更にフレキシブルに接続自在なコンピュータ・システムの一つに接続するため移動ユーザからＦＣＣＳプラグを受容すると共に機密情報を用いて少なくとも一つのコンピュータ動作を行い、これにより機密性を増強させるステップを含む方法。

【００２２】好ましくは、前記の装置は、ＵＳＢインタフェースからＵＳＢ通信を受容してそれに対する計算を行うと共に計算の結果をデータ記憶ユニットに与えて記憶し、および／または暗号化し、および／または認証し、および／またはアクセス制御するように動作するマイクロプロセッサをさらに含む。

【００２３】用語「ＵＳＢポート」は、ｗｗｗ．ｕｓｂ．ｏｒｇでインターネットから得られるＵＳＢ仕様に記載されたＵＳＢ標準に従って得られたコンピュータに周辺装置を接続するポートに関係する。

【００２４】用語「ＵＳＢプラグ」または「ＵＳＢキー」または「ＵＳＢトークン」は、回路がＵＳＢポートとインタフェースして各種の機能を実行するハードウエア装置に関係する。

【００２５】用語「スマート・カード」は、チップが埋設された通常のプラスチックのカードであり、このチップ

はリーダと対話し、これにより、スマート・カードの移動保有体が、スマート・カード・リーダを設置している機械、通常この種の機械のネットワークのいずれかと対話することを可能にするものである。

【００２６】更に、本発明の好適な実施例によれば、ＰＣ、ラップトップ、パルムトップ、または周辺装置などの任意のコンピュータ・システムのＵＳＢポートなどのフレキシブル接続を与えるポートと好適に連接する電子トークンが与えられる。電子トークンは、好適には何らかの付加的な読み取り装置を必要としない。トークンは、家庭のハウス・キーの大きさでもよいトークンにおいて、情報を認証し、および／またはパスワードまたは電子証書を記憶してもよい。

【００２７】好適には、フレキシブルな接続を与えるポートにトークンが挿入されると、充分に確実な「二重因子認証（ｄｕａｌ　ｆａｃｔｏｒ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ）」プロセス（例えば、「あなたが持つもの」プラス「あなたが知ること」）が行われ、そこでは、（ａ）電子トークンが、ホストＰＣＣまたはネットワークにより読み取られ、（ｂ）ユーザが、許可のための彼の、または彼女の個人的パスワードにタイプする。

【００２８】電子トークンに対する適切な応用には、ＶＰＮ、エクストラネットおよびｅ－ｃｏｍｍｅｒｃｅに対する認証がある。本発明は更に、改良されたＵＳＢ装置を提供し、またそれを用いる改良された方法を提供する。

【００２９】このようにして、本発明の他の好適な実施例によれば、ＵＳＢポートを介してＵＳＢホストと対話するＵＳＢキー装置が提供され、このＵＳＢキー装置は、ＵＳＢポートに適合するように構成されたポータブル装置を備え、このポータブル装置は、ＵＳＢホストに、およびＵＳＢホストから、ＵＳＢ通信を搬送するＵＳＢインタフェースを備え、更にＵＳＢキー装置は、ＵＳＢプロトコルからのＵＳＢ通信を、ＩＳＯ７８１６プロトコルのようなスマート・カード・プロトコルに翻訳し、またスマート・カード・プロトコルをＵＳＢプロトコルに翻訳するように動作するプロトコル・トランスレータを備え、更に認証、暗号化、アクセス制御などの少なくとも一つのスマート・カード機能を行うと共にメモリを確保するように動作するスマート・カード・チップを備える。

【００３０】更に、本発明の他の好適な実施例によれば、データ記憶能力を有するＵＳＢキー装置が提供され、このＵＳＢキー装置は、ＵＳＢポートに適合するように構成された、ＰＣＢなどのポータブル装置を備え、このポータブル装置は、ＵＳＢホストに、およびＵＳＢホストから、ＵＳＢ通信を搬送するＵＳＢインタフェースと、ＵＳＢ通信から導出された情報を記憶するデータ記憶ユニットとを備える。

【００３１】

【好適な実施例の詳細な説明】図１を参照すると、ＣＰＵとノン（ｎｏｎ）-ＩＳＯ７８１６メモリを備え、本発明の好適な実施例に従って構成され、動作するフレキシブルに接続自在なＵＳＢプラグ装置の概略ブロック図が示される。

【００３２】図１のＵＳＢプラグ装置の特徴は、それがデータ記憶機能を有し、従ってメモリ・スマート・カードに類似する点にある。ＵＳＢプラグ装置１０は、ＰＣＢ２５からなり、これは、モトローラ６８０５、ＣｙｐｒｅｓｓチップまたはＩｎｔｅｌ８０５１などのマイクロプロセッサまたはＣＰＵ３０と、ＵＳＢインタフェース装置（チップ）４０と、マイクロプロセッサ３０のファームウエアをセーブするファームウエア・メモリ５０と、マイクロプロセッサ３０の一部において意図された計算を可能にするのに十分な大きさのＲＡＭメモリ６０と、更にユーザのデータを記憶するユーザ・データ・メモリ７０とを備えている。ＵＳＢインタフェース装置４０、ファームウエア・メモリ５０、およびＲＡＭメモリ６０の幾つかまたは全ては、ＣＰＵ３０内に配置してもよい。

【００３３】ＵＳＢインタフェース装置４０および／またはファームウエア・メモリ５０は、マイクロプロセッサ３０内に統合してもよい。ファームウエア・メモリは、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、またはＦＬＡＳＨなどの、しかしそれらに限定はされない適切な種類のメモリであってもよい。

【００３４】ユーザ・データ・メモリ７０は、通常ＩＳＯ７８１６－３メモリは備えず、例えば、次の種類のメモリ：I^2C、ＸI^2C、２／３ワイアバス，ＦＬＡＳＨなどのいずれかを含む。

【００３５】図示のように、ＵＳＢプラグ装置１０は、ＵＳＢポートを有するパーソナル・コンピュータまたはＭａｃｉｎｔｏｓｈなどの、しかしそれらに限定はされない任意のＵＳＢホストと対話するように構成される。キーとホスト間の対話は、ｗｗｗ．ｕｓｂ．ｏｒｇ．でインターネットから得られるＵＳＢ仕様に示されたＵＳＢプロトコルのような、ＵＳＢプロトコルにより支配される。ＵＳＢパケットは、ＵＳＢホスト２０とＵＳＢインタフェース・チップ４０の間を通過する。各パケットは、通常次の要素を備える。

ａ．　ＵＳＢヘッダ；

ｂ．　ユーザのデータ・メモリ７０に対して記憶／読み出しされるデータと、データを記憶し／読み出すアドレス、記憶／読み出すデータの長さ、ＣＲＣチェックサム情報などの、しかしそれらに限定はされないメモリ・チップ７０のプロトコルにより要求される付的情報；

ｃ．　ＵＳＢフッタ。

【００３６】データの流れは、通常次の流れを含む。ＵＳＢインタフェース・チップ４０は、ＵＳＢホスト２０からＵＳＢパケットを受け、データを分析し、分析した

データをマイクロプロセッサ３０に送出する。マイクロプロセッサ３０は、各メモリのプロトコルを用いて、ファームウエア・メモリ５０、ＲＡＭ６０、またはユーザのデータ・メモリ７０にデータを書き込み、またはそれからデータを読み出す。

【００３７】読み取り動作時には、マイクロプロセッサ３０は、データをＵＳＢインタフェース・チップ４０に送出し、このチップは、データをＵＳＢパケット・フォーマットにラップし、これをホスト２０に送出する。

【００３８】図２は、本発明の好適な実施例に従って構成され、動作するＵＳＢプラグ装置の概略ブロック図であり、これは、好適には共に確保された記憶および暗号能力を与えるスマート・カード・チップおよびワンピースのスマート・カード・リーダである。図２のＵＳＢプラグ装置は、ＣＰＵと、スマート・カード・チップ（ＩＣＣ）メモリ１７０を共に備え、通常ＩＳＯ７８１６-３プロトコルを用いてＣＰＵ１３０と通信するＩＳＯ７８１６（Ｔ＝０／１）プロトコル・ベースのチップである。図２の装置は、別個のユーザ・データ・メモリ７０が設けられていないことを除いて、図１の装置に類似している。ＲＡＭ１６０の大きさは、通常ＩＳＯ７８１６-３　Ｔ＝０またはＴ＝１　プロトコルを保有するために、通常少なくとも２６２バイトである。

【００３９】各パケットは、通常以下の要素を備える。

ａ．　ＵＳＢヘッダ；

ｂ．　ＩＳＯ７８１６－３　Ｔ＝０／１プロトコル・パケット；

ｃ．　ＵＳＢフッタ。

【００４０】図２の装置におけるデータの流れは、次の流れを含む。ＵＳＢインタフェース・チップ１４０は、ＵＳＢホスト１２０からＵＳＢパケットを得る。ＵＳＢインタフェース・チップ１４０は、データを分析し、それをマイクロプロセッサ１３０に送出する。通常、ＩＳＯ７８１６－３　Ｔ＝０／１フォーマット・パケットを含むデータが、ＩＳＯ７８１６－３プロトコルでスマート・カード１７０にマイクロプロセッサにより送出される。マイクロプロセッサ１３０はスマート・カード１６０から応答を得、このデータをＵＳＢインタフェース・チップ１４０に送出する。ＵＳＢインタフェース・チップ１４０は、データをＵＳＢパケット・フォーマットでラップし、それをホスト１２０に送出する。

【００４１】図２の実施例の利点は、スマート・カードの機能が与えられるが、プラグ１１０がホスト１２０のＵＳＢソケットに直接接続されるために専用のリーダの必要性がないという点にある。

【００４２】ここに図示し且つ説明した発明は、銀行、保険会社、会計事務所および他の商業機関などの機密情報を処理する機関、および医療機関または法律機関などの職業的な機関に供給するコンピュータ化されたシステムに対して特に有用である。

【００４３】従来のコンピュータ・システムには、コンピュータ（マザーボードを含む）および少なくとも一つの周辺装置がある。このコンピュータは、各種周辺装置のポートに連接する多数の異なるポートを有する。各ポートは、通常特定の周辺装置のみに連接できるが、他の周辺装置とは連接できない。例えば、キーボードは、コンピュータのプリンタ・ポートを介して、コンピュータに接続することはできない。

【００４４】現在のコンピュータ・システムにおいては、「フレキシブルに接続自在なコンピュータ・システム」とも呼ばれるが、コンピュータおよび周辺装置はそれぞれ、任意の周辺装置が任意のコンピュータまたは任意の他の周辺装置に選択可能に接続できるように、任意のコンピュータおよび任意の他の周辺装置の連接ポートを有する少なくとも一つの同等のポートを備える。更に、周辺装置は、従来のシステムにおけるように直接ではなく、むしろ他の周辺装置を介して、コンピュータに接続されてもよい。他の周辺装置が一般的に常に既存のコンピュータ・システムに接続できるように、既存のコンピュータ・システムにおける一つまたはそれ以上の接続された周辺装置で利用可能なポートが一般的に常に得られる。

【００４５】フレキシブルに接続自在なコンピュータ・システムの一例は、ＵＳＢ（汎用標準バス：Ｕｎｉｖｅｒｓａｌ　Ｓｔａｎｄａｒｄ　Ｂｕｓ）システムであり、このシステムでは，コンピュータおよび各周辺装置はＵＳＢポートを有する。フレキシブルに接続自在なコンピュータ・システムの他の例は、最近意図されたファイアワイア・システムである。

【００４６】「ＵＳＢプラグ」は、ＵＳＢシステムに連接するポータブル装置であり、機械的素子を含む周辺装置に対抗するように、通常メモリおよび／またはＣＰＵのみからなり、従って通常ポケットサイズである。より一般的には、ＵＳＢプラグは、フレキシブルに接続自在なコンピュータ・システム（ＦＣＣＳ：Ｆｌｅｘｉｂｌｙ　Ｃｏｎｎｅｃｔｉｂｌｅ　Ｃｏｍｐｕｔｅｒ　Ｓｙｓｔｅｍ）にプラグ接続されるプラグの例である。

【００４７】ここで、「ＵＳＢプラグ」という用語は、フレキシブルに接続自在なコンピュータ・システムと連接し、且つ機械的素子を含む周辺機器に対立するものとして、通常メモリおよび/またはＣＰＵのみを含み、従って、それは通常ポケットサイズである。フレキシブルに接続自在なコンピュータ・システムに接続された各周辺装置は通常少なくとも一つのポートを有するため、任意の構成のフレキシブルに接続自在なコンピュータ・システムは、ＦＣＣＳプラグと対話するために得られる少なくとも一つの空きポートを通常有することが認められている。ＵＳＢトークンおよびＲａｉｎｂｏｗトークンは共にＦＣＣＳプラグの例である。

【００４８】通常、コンピュータ・システムを形成する

複数個のコンピュータ・システム・ユニット（コンピュータおよび一つ以上の周辺装置）の各々は、少なくとも二つの同等の雌ソケットを有し、これらは雄ー雄ケーブルにより相互に接続される。本実施例においては、ＦＣＣＳプラグは雄ソケットを含む。しかし、任意の適切な連接スキームを用いて、コンピュータ・システム・ユニットと本発明のＦＣＣＳプラグとを連接させてもよいことが認識される。

【００４９】ＦＣＣＳプラグの既知の用途は、プラグ認識能力を有するソフトウエアと関連して使用するものである。ＡｌａｄｄｉｎおよびＲａｉｎｂｏｗの両者は、特定のソフトウエアが存在するホスト・コンピュータ・システムがソフトウエア・コピーにより認識されるＦＣＣＳプラグに挿入されるときにのみ動作するソフトウエアを市販している。ＡｌａｄｄｉｎおよびＲａｉｎｂｏｗのプラグは認証には用いられない。

【００５０】コンピュータ・システムは、一群の移動ユーザである一つの移動ユーザを特徴づける情報を受信し、更にこの情報を処理するために度々用いられる。このような情報は、ユーザの一致の認証情報、銀行手続情報、アクセス権情報などを含む。従来、この情報はユーザにより保有され、彼によりコンピュータ・システムに提供されるスマート・カードに記憶される。しかし、これは、コンピュータ・システムがスマート・カード・リーダ、すなわちスマート・カードを読み取ることを専用とする特殊な装置片を備えることを要求する。

【００５１】本発明の好適な実施例によれば、移動ユーザを特徴づける情報はＦＣＣＳプラグに記憶される。本発明のこの実施例の利点は、情報がポケットサイズの基板にユーザにより容易に保有されること、任意の構成のフレキシブルに接続自在なコンピュータ・システムがＦＣＣＳプラグを介してユーザと通常対話することができること、更に対話を実施するのに専用の装置がコンピュータにより要求されないこと、にある。

【００５２】図３を参照すると、本発明の好適な実施例に従って構成され、動作し、図１のＵＳＢキー装置を実施するＦＣＣＳプラグの展開前面図が示されている。図示のように、図３のＦＣＣＳプラグは、図１のＵＳＢコネクタ２２０およびＰＣＢ２５が間に配置される二つのスナップ結合の平面カバー素子２００と２１０で通常形成されたハウジングを含む。ＵＳＢコネクタ２２０は、例えば、Ａｓｋａ　Ｔｅｃｈｎｏｌｏｇｉｅｓ社，Ｎｏ．１５、Ａｌｌｅｙ２２、Ｌａｎｅ２６６、Ｆｕ　Ｔｅｈ,１ｓｔ Ｒｄ.,Ｈｓｌ Ｃｈｉｈ,Ｔａｌｐｅｉ Ｓｈｉｅｎ,Ｔａｉｗａｎ所在、により市販されているＵＳＢ　ＰＬＵＧ　ＳＭＴ<ＡＣＮ-０２１３>装置から構成してもよい。ＰＣＢ２５は、図１の各素子３０、４０、５０、６０および７０を保有する。メモリ２４０を管理するファームウエアは、ＵＳＢインタフェース制御装置２３０に配置してもよい。

【００５３】図４を更に参照すると、本発明の好適な実施例に従って構成され、動作し、図２のＵＳＢキー装置を実施するＦＣＣＳプラグの展開図が示されている。図示のように、図４のＦＣＣＳプラグは、ＵＳＢコネクタ２２０とＰＣＢ１２５が間に配置された二つのスナップ結合の平面カバー素子２００と２１０で通常形成されたハウジングを含む。ＰＣＢ１２５は、図２の各素子１３０、１４０、１５０、１６０および１７０を保有する。スマート・カード・チップ２５０を管理するファームウエアは、ＵＳＢインタフェース制御装置２３０に配置される。

【００５４】本発明のＦＣＣＳプラグにより好適に与えられるスマート・カード機能には、次のものがある。

１．コンピュータ・ネットワークへのアクセスを制御する。スマート・カードまたはプラグは、ＩＤ情報、ネットワーク認証を有し、それに基づくアクセスを可能にする。認証は、「あなたは何を持つか」、例えばバイオメトリック情報の「あなたは何であるか」、および「あなたは何を知っているか」、（例えばパスワード）、に基づくものであってよい。

２．ドキュメントの送り主の一致を検証または認証するためのデジタル署名または証明。

３．機密情報、例えば医療情報の記憶。スマート・カードまたはプラグは、機密情報を記憶し、機密情報を記憶しないネットワークと対話する。図５Ａ－５Ｂは、フレキシブルに接続自在な一群のコンピュータ・システム３００および一群の移動ユーザにより使用するための本発明の好適な実施例に従って与えられる、ユーザとコンピュータ間の対話方法を図式的に示したものである。各移動ユーザを特徴づける情報、例えば名前とＩＤは、通常、図３のユニット２３０のようなＵＳＢインタフェース制御装置を介して、その移動ユーザにより保有されるＦＣＣＳプラグ３１０のメモリにロードされる。

【００５５】次に、プラグは、フレキシブルに接続自在のコンピュータ・システムの一つに、および、認証のような従来のスマート・カードの機能を通常含む少なくとも一つのコンピュータ動作を行うために使用される移動ユーザを特徴づける情報に、接続可能である。

【００５６】本発明の好適な実施例の特徴をここで説明する。

【００５７】ａ．増強したユーザ認証の必要性

＊認証は、任意の情報セキュリティー・システムに対する基本である。ローカルおよびリモート・ユーザを認証する能力は、ＬＡＮ／イントラネット、マルチユーザ環境に対して重大な問題である。

ｂ．暗号化および機密性の必要性

＊内容の暗号化および機密性は、団体および個別ユーザに対して重要な問題になる。

ｃ．パスワードおよびサインーオン（Ｓｉｇｎ－Ｏｎ）のセキュリティー

＊パスワードのセキュリティーおよびユーザ・パスワードの管理は、ネットワークの団体ユーザにとって主要な問題である。パスワードは、任意の計算環境において単一の最も重要なセキュリティー関係を表す。

【００５８】今日、ハードウエア・ベースのＰＣセキュリティー・トークンに対する必要性がある。

＊ サイン-オン-キー（ＳＯＫ：Ｓｉｇｎ－Ｏｎ－Ｋｅｙ）は、ハードウエア・ベースのトークンであり、Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍｓ&Ａｐｐｌｉｃａｔｉｏｎｓとシームレスに統合して、

-ユーザ認証キーと、

-暗号化システムに対するベースと、

-より良好なサイン－オン・セキュリティーおよび増強したユーザ・パスワード管理と、

－ソフトウエア・セキュリティーと、

を与える。

認証-３つの基本要素

＊あなたが知る何か　——>パスワード

＊あなたが持つ何か　——>サイン－オン－キー

＊あなたが何か　——>例えば、バイオメトリック（Ｂａｉｏ－ｍｅｔｒｉｃｓ）

＊ 仮定：前記三つの内の二つが「良好で充分な」セキュリティーを与える。

【００５９】暗号化

＊ データ、ファイル、ディスク、および情報流を暗号化する必要性は明らかである。

＊ 暗号化能力を有するハードウエア・ベースのトークンは、セキュリティーと使用の容易性とを増強することができる。

【００６０】サイン－オン、どこでパスワードが使用されるか？

＊ あなたのＯ／Ｓに対してログ・オン

＊ あなたのネットワーク（ローカル、リモート）に対してログ・オン

＊ インターネット／ＩＳＰに対してログ・オン

＊ 保護されたウエブ・ページに対してログ・オン

＊ グループ・ウエア／通信アプリケーションに対してログ・オン

＊ 他の機密パスワード保護アプリケーションに対してログ・オン

＊ ＭＳ　Ｏｆｆｉｃｅ&他の保護ファイル

＊ ＰＣブート保護（Ｂｉｏｓパスワード）

【００６１】サイン－オン、主要なセキュリティー・リスク

サイン－オン・プロセス

サイン－オン－キーは、要求されたアプリケーションに対してユーザによりリンクされた、セキュリティー・ハードウエア・トークンである。インストールすると、サイン－オン－キーは、ログ・オンのプロセスの一部になる。サイン－オン－キーは、セキュリティーおよび他の機能的な多くの利点をユーザに与える。

【００６２】サイン－オン－キーはユーザのために何をすることができるか？

＊ サイン－オン　セキュリティー

－ 増強セキュリティー&認証。　サイン－オン－キーがユーザパスワードに加えて要求される。

＊ サイン－オン　容易性

－ログ・オンのプロセスを簡単にし、パスワードに対する必要性を排除する。サイン－オン－キーがパスワードを置き換える。

＊ パスワードの自動再検証

-サイン－オン－キーを定期的にチェック

＊ 単一のサイン－オン

－一つのサイン－オン－キーが、幾つかのアプリケーションに対して幾つかのパスワードを置き換える。

＊ モビリテイ&リモート計算

-サイン－オン-キーは、リモート・ユーザを識別する。

-サイン-オン－キーをデータ確保容器として用いることができる。

-移動ＰＣの盗難防止

＊ 汎用セキュリティー・トークン

-ファイル&データ暗号化

-認証

-証明キー・ホルダー

【００６３】サイン－オン－キーの各種オプシヨン

＊ 幾つかのハードウエア装置は、サイン－オン－キーとして動作してもよい。

-サイン－オン－キーＵＳＢ－　新しい標準ＵＳＢポートに接続する小さなキー。ＵＳＢポートは、ＰＣおよびＭａｃｉｎｔｏｓｈに対して新しい接続標準になりつつある。

-サイン－オン－キー・ＳＣ－　スマート・カード・ベースのサイン－オン－キー。任意の標準スマート・カード・ドライブと共に使用できるか。

【００６４】サイン－オン－キー・ＵＳＰ&利点

＊ 単純，直感的，使用が容易、魅惑的トークン

＊ キーは、トークンがコネクタであるということである。

＊ 低価格

＊ 高いセキュリティー

＊ 高い機能性

－メモリ・インサイド・トークン

-処理能力

-自動パスワード再検証

-多重トークン接続性

＊ エイジェントのソリューシヨン

【００６５】サイン－オン－キーのアーキテクチャ

フル・ブラウン・システム

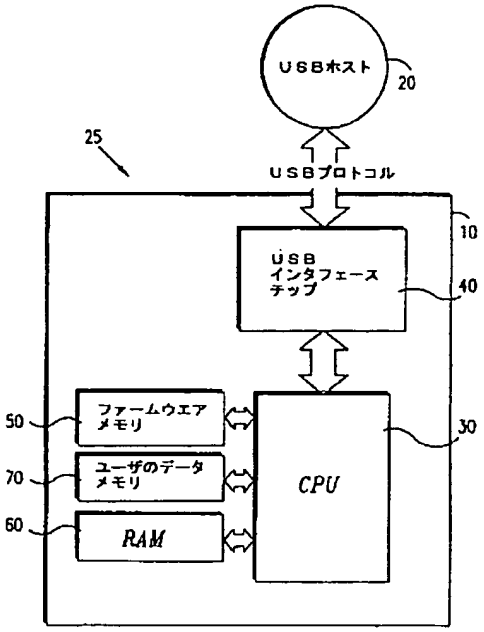
サイン　オン　エイジェント

＊ サイン－オン-エイジェント（Ｓｉｇｎ－Ｏｎ－Ａｇ

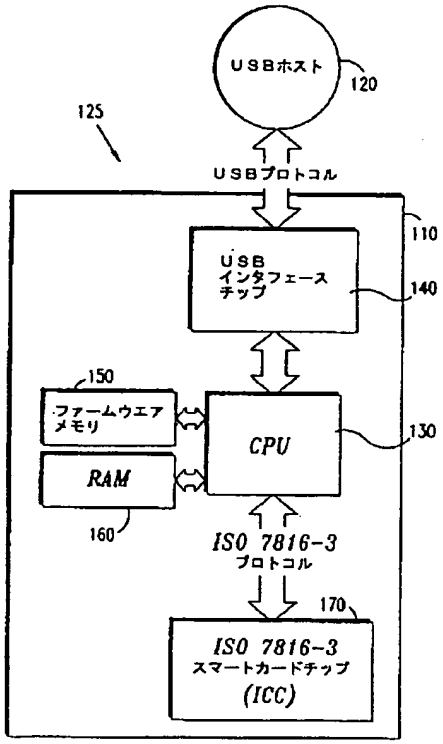
ｅｎｔ）は、サイン－オン－キーとアプリケーションとの間のソフトウエア・インタフェースである。
＊ サイン－オン－ブート（Ｓｉｇｎ－Ｏｎ－Ｂｏｏｔ）は、ＰＣブート・パスワードに対する特殊なインタフェースである。
＊ エイジェントは以下に対して与えられる。
－ＯＳ／ネットウエア、例えば、ＷｉｎｄｏｗｓＮＴ、９５／９８、３ｘ、Ｎｏｖｅｌ、Ｕｎｉｘ
-グループウエア／メール、例えば、Ｌｏｔｕｓ Ｎｏｔｅｓ、Ｏｕｔｌｏｏｋ、Ｅｕｄｏｒａ
－エンタプライズ アプリケーション、例えば、ＳＡＰ、Ｂａａｎ，ＭＫ、Ｏｒａｃｌｅ，Ｍａｇｉｃ
-ウエブ ブラウザ、例えば、Ｅｘｐｌｏｒｅｒ、Ｎａｖｉｇａｔｏｒ
【００６６】最もトリビヤルなエイジェント-ＷｉｎｄｏｗｓＮＴ
＊ 最もトリビヤルなエイジェントは，Ｗｉｎｄｏｗｓ Ｌｏｇｉｎ セッションを置き換える。
＊ そうすることによりユーザは次のものを得る。
-Ｗｉｎｄｏｗｓ Ｌｏｇｉｎ Ｅｘｔｒａ セキュリティー
－Ｗｉｎｄｏｗｓ Ｌｏｇｉｎの単純化（サイン－オン－キーはパスワードを置き換える）。
【００６７】サイン-オン－キー ウエブ・ブラウザのエイジェント／システム
＊ サイン-オン-キーは、確保されたウエブ・ページへのアクセスをモニタする認証トークンとして用いることができる。
＊ ウエブ・コンテント・プロバイダは、彼らのカスタマへのアクセスを、認証し、管理し、与える必要がある。
【００６８】サイン－オン-キー・ＡＰＩ（ＳＤＫ）
＊ サイン－オン－キー・ＡＰＩは、サイン－オン－キーと第三者のアプリケーションとの間のインタフェース・レベルである。
＊ このＡＰＩは、証明プロバイダ、セキュリティー会社、ＳＳＯ会社による処理に対して公表され、オープンにされる。
＊ サイン－オン－キー・ＡＰＩはまた、暗号化&保護メモリ記憶サービスを与える。
＊ サイン-オン-キー・ＡＰＩは、ＰＫＣＳ＃１１ベース／コンパチブルである。
【００６９】サイン-オン・プロセス（Ｎｏ ＣＡ）
＊ インストール
-ユーザは、要求されたアプリケーションに対してエイジェントをインストールする。
-ユーザは、各アプリケーションに対してサイン-オン・パラメータを規定する。
-ユーザは、サイン－オン－キーにサイン-オン情報を記憶する。
＊ サイン－オン
-アプリケーションが開始される。
-アプリケーションは、そのサイン-オン・ダイアローグに達する。
-アプリケーションは、サイン-オン－キーと通信する。
-サイン-オン・パーミッションが、サイン-オン－キーに基づいて認められる。
【００７０】確実な容器としてのサイン-オン-キー
＊ 独自のキーＩＤに加えて、サイン-オン-キーは、個人保護メモリ領域を収容する。
＊ このメモリ領域は、機密情報と証明とを記憶するために使用することができる。
＊ Ｌｏｔｕｓ Ｎｏｔｅｓ ＩＤファイルまたはＰＧＰキーのようなアプリケーションのＩＤキーがこのメモリに記憶され得る。
＊ そうすることで、 サイン－オン-キーを用いて移動計算のセキュリティーを増加させることができる。ファイルＩＤは、ディスクの代わりにサイン-オン-キーに記憶される。
【００７１】サイン-オン-キー 暗号化エンジン&サイン-オン-キー・クリプト（Ｃｒｙｐｔ）
＊ サイン-オン－キーは、暗号化装置として用いることができる。
＊ 暗号化ＡＰＩが設けられ、例えば、１００％スマート・カード互換のサイン-オン-キーの実施
＊ サイン-オン-キー・クリプトは、サイン-オン-キーに基づくデータ／ファイル／ハードディスク暗号化ユティリテイである。
【００７２】サイン-オン-キー証明ツールキット
＊ ＳＯＫは、ＰＫＣＳ＃１１およびＸ５０９を用いてよく、また証明および／またはデイジタルＩＤを記憶してもよい。
【００７３】サイン-オン-キーは次のものを含む。
＊ サイン-オン-キーＵＳＢトークン
＊ ＨＡＳＰ
＊ ハードロック
＊ 初期サイン-オン-キー機能性（独自のＩＤ、個人保護メモリ）
＊ サイン-オン-キーＵＳＢ拡張ケーブル
＊ サイン-オン-キー・スマート・カード・トークン
＊ サイン-オン-キー・ＡＰＩ（ＰＫＣＳ＃１１コンプライアント）
＊ エントラスト・コンパテビリテイ／リンク
＊ ＷｉｎｄｏｗｓＮＴ Ａｇｅｎｔ
＊ Ｎａｖｉｇａｔｏｒおよび／またはＥｘｐｌｏｒｅｒ Ａｇｅｎｔ（Ｓ／Ｍｉｍｅ）
＊ Ｋｅｙ Ｐｌｕｓ Ｃｒｙｐｔ（Ｂｅｔａリリース）
＊ 確実なスクリーン・セーバ
＊ 初期のマーケッテイング・パッケージ

＊ USBの拡散&Windows98／NTの有効性が主要な問題である。
＊ US、ドイツ&イスラエルにおいては、全ての新しい出荷PCは、USBを備えている。
＊ 初期開発段階におけるセクシヨン化
＊ Security Dynamics, Activ Card & Vascoは、第一世代の時間ベース・ワンタイム・パスワードまたはチャレンジ・ベースのトークンにより、マーケットを制御する。
＊ セキュリティー・ベンダーは、クリプトグラフィ、デイジタル署名記憶および処理動作をサポートする第二世代の統合スマート・カードのオファリングと共にそれらの市場シェアを拡大する。
【0074】USB：より良好な接続
＊ ほとんど無制限のポートの拡張
＊ 新しい周辺装置に対するアッドーイン・カード無し
－IRQ、DMAなどの設定無し
＊ 一つの接続タイプ（プラグおよびポート）
－多くの周辺装置
－より多くのゲスワーク（当てずっぽう）無し
－単純な設定、正確なプラグ・インおよび作動
【0075】USB：より良好な接続
＊ アドレスは、速度、多重媒体を必要とする
－12Mb／s、Asynch（バルク）＆Isoch（リアル・タイム）データ
－ステレオー 良質なデジタル・オーデイオ
－高いフレーム・レート・ビデオ（圧縮付き）
－高い持ち時間のアプリケーシヨン（強制フィードバック）
＊ 多くの新しい周辺装置に伴うパワー・ブリック無し
－USBは500mAまで供給
＊ PCユーザの経験が大いに改善される。
－僅かな返品とセールス・ポテンシヤルの増加。
【0076】USBはフレキシブルな接続標準の単なる一例であり、本発明はUSBに限定されるものではないということが明らかである。
【0077】本発明のソフトウエア成分は、所望ならば、ROM（リード・オンリ・メモリ）形態で実施されるということが明らかである。ソフトウエア成分は、所望ならば、従来の技術を用いて、一般的にはハードウエアで実施されてもよい。
【0078】明瞭にするために、個別の実施例により記述された本発明の各種の特徴はまた、単一実施例の組み合わせで与えられてもよいということが明らかである。逆に、簡単のため、単一の実施例により記述される本発明の各種の特徴はまた個別に、または任意の適切な副次的組み合わせで与えられてもよい。
【0079】本発明は以上において特別に図示、説明されたものに限定されるものではないということは当業者には明らかである。むしろ、本発明の範囲はクレームによってのみ規定される。
【図面の簡単な説明】
【図1】図1は、CPUとノンーISO7816メモリを備え、本発明の好適な実施例に従って構成され、動作するUSBプラグ装置の概略ブロック図である。
【図2】図2は、CPUとISO7816メモリを備え、本発明の好適な実施例に従って構成され、動作するUSBプラグ装置の概略図である。
【図3】図3は、本発明の好適な実施例に従って構成され、動作し、図1のUSBプラグ装置を実施するFCCSプラグの展開前面図である。
【図4】図4は、本発明の好適な実施例に従って構成され、動作し、図2のUSBプラグ装置を実施するFCCSプラグの展開図である。
【図5】図5Aおよび図5Bは、フレキシブルに接続自在な一群のコンピュータ・システムおよび一群の移動ユーザにより使用される本発明の好適な実施例に従って与えられる、ユーザとコンピュータ間の対話方法を図式的に示す図である。

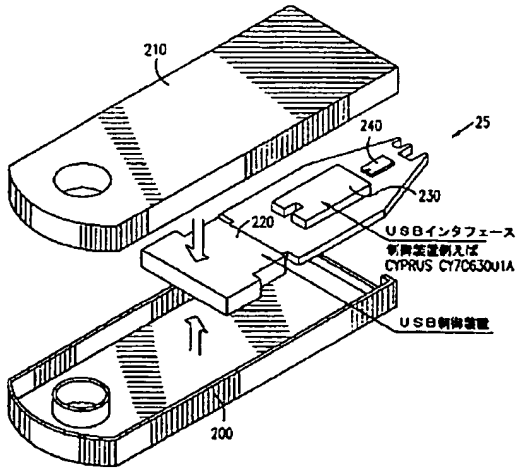
【図１】


USBホスト
20
25
USBプロトコル
10
USB
インタフェース
チップ
40
ファームウエア
メモリ
50
ユーザのデータ
メモリ
70
RAM
60
CPU
30

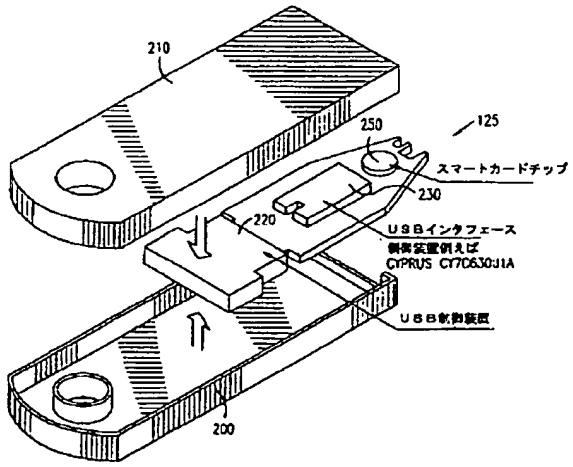
【図２】


USBホスト
120
125
USBプロトコル
110
USB
インタフェース
チップ
140
150
ファームウエア
メモリ
RAM
160
CPU
130
ISO 7816-3
プロトコル
170
ISO 7816-3
スマートカードチップ
(ICC)

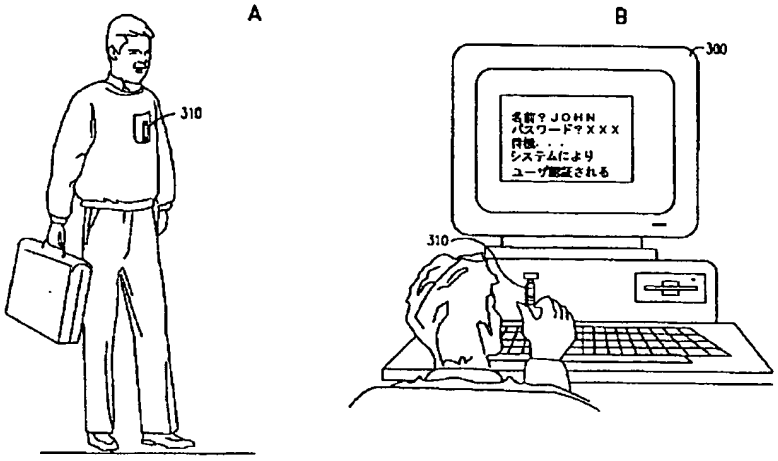
【図３】


210
240
25
230
220
USBインタフェース
CYPRUS CY7C630U1A
200

【図４】


210
250
125
スマートカードチップ
230
220
USBインタフェース
CYPRUS CY7C630U1A
200

【図５】



フロントページの続き

(72)発明者　ラミ・カステルシュティエン
イスラエル国テル・アビブ　67442，ナハ
ラト・イズハク・ストリート　37

【外国語明細書】

1. Title of Invention

USER-COMPUTER INTERACTION METHOD AND APPARATUS

2. Claims

1. A user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method comprising:

storing information characterizing each mobile user on an FCCS plug to be borne by that mobile user; and

accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the information characterizing the mobile user to perform at least one computer operation.

2. A method according to claim 1 wherein said at least one computer operation comprises authentication.

3. An FCCS plug device to be borne by a mobile user, the FCCS plug device comprising:

a portable device which mates with a flexibly connectible computer system and comprises a memory; and

information characterizing the mobile user and stored in said memory accessibly to the flexibly connectible computer system.

4. A population of FCCS plug devices to be borne by a corresponding population of mobile users, the population of FCCS plug devices comprising:

a multiplicity of portable devices each of which mates with a flexibly connectible computer system and comprises a memory; and

information characterizing each mobile user in the population of mobile users and stored, accessibly to the flexibly connectible computer system, in the memory of the FCCS plug device to be borne by said mobile user.

5. An FCCS plug device comprising:

a mating element operative to mate with a flexibly connectible computer system; and

a memory connected adjacent said mating element, thereby to form a portable pocket-size plug, wherein the memory is accessible to the flexibly connectible computer

system via said mating element.

6. An FCCS plug device comprising:

a mating element operative to mate with a flexibly connectible computer system; and

a CPU connected adjacent said mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via said mating element.

7. An FCCS plug device according to claim 5 and also comprising a CPU connected adjacent said mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via said mating element.

8. A method according to claim 1 wherein said at least one computer operation comprises digital signature verification.

9. A method according to claim 2 wherein said at least one computer operation comprises controlling access to computer networks.

10. A method according to claim 1 wherein said information characterizing each mobile user comprises sensitive information not stored in said computer system, thereby to enhance confidentiality.

11. A user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method comprising:

storing confidential information not stored by the flexibly connectible computer systems on an FCCS plug to be borne by an individual user within said population of mobile users; and

accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the confidential information to perform at least one computer operation, thereby to enhance confidentiality.

12. USB key apparatus for interacting with a USB host via a USB port, the USB

key apparatus comprising:

a portable device configured to fit the USB port, the portable device comprising:

a USB interface conveying USB communications to and from a USB host;

a protocol translator operative to translate the USB communications from USB protocol into smart card protocol and from smart card protocol into USB protocol; and

a smart card chip operative to perform at least one smart card function.

13. USB key apparatus according to claim 12 wherein the smart card protocol comprises an ISO7816 protocol.

14. USB key apparatus with data storage capabilities, the USB key apparatus comprising:

a portable device configured to fit a USB port, the portable device comprising:

a USB interface conveying USB communications to and from a USB host; and

a data storage unit storing information derived from the USB communications.

15. Apparatus according to claim 12 wherein the smart card function comprises at least one function selected from the group consisting of secured memory, authentication, encryption and access control.

16. Apparatus according to claim 14 and also comprising a microprocessor operative to receive said USB communications from the USB interface, to perform computations thereupon and to provide results of the computations to the data storage unit for storage.

17. A method for interacting with a USB host via a USB port, the method comprising:

configuring a portable device to fit the USB port;

conveying USB communications to and from a USB host;

translating the USB communications from USB protocol into smart card protocol and from smart card protocol into USB protocol; and

providing a smart card chip operative to perform at least one smart card function.

18. A method according to claim 17 wherein the smart card protocol comprises an ISO7816 protocol.

19. A data storage method comprising:

configuring a portable device to fit a USB port;

conveying USB communications to and from a USB host; and

storing information derived from the USB communications.

20. A method according to claim 17 wherein the smart card function comprises at least one function selected from the group consisting of secured memory, authentication, encryption and access control.

21. A method according to claim 19 and also comprising employing a microprocessor to receive said USB communications from the USB interface, to perform computations thereupon and to provide results of the computations to the data storage unit for storage.

3. Detailed Description of Invention

FIELD OF THE INVENTION

The present invention relates to flexibly connectible computer apparatus and methods for using flexibly connectible hosts.

BACKGROUND OF THE INVENTION

The USB interface is described in specifications available over the Internet at www.usb.org.

Firewire technology, also termed "IEEE 1394 technology", is an alternative to USB which also provides flexible connectivity and is described in the IEEE 1394 standard.

USBHasp is an Aladdin software protection product, announced in October 1997, which includes a USB key. USBHasp does not control access of a user to a computer network but rather impedes interaction between software and a computer system by activating a copy of the software only if a USB key corresponding to that copy is plugged into the computer system.

Conventionally, the only devices which have interacted via USB have been computers, keyboard, monitor, printer, mouse, smart card readers, and biometric readers.

Conventional devices for providing computerized servicing to a mobile or stationary population of users typically include a smart card reader. The members of the mobile population bear smart cards which are used to interact with the computerized servicing device via the smart card reader.

A particular disadvantage of smart cards is that they require a smart card reader which is a relatively costly device. Computer hosts which are equipped with a smart card reader are a small subset of the universe of computer hosts because addition of a smart card reader makes the computer considerably more expensive.

German Patent document DE 19631050 describes an interface converter for a universal serial bus having a module with a processor that changes format and protocol into that of a different bus system.

Rainbow Technologies, Inc., in a news release dated 17 November 1998, announce USB software protection keys which can also be used as authentication or access

control devices. A unique ID number if assigned to each USB key, enabling the key to replace or supplement personal passwords.The unique ID of the USB key makes it useful as a notebook computer security device providing theft deterrence. Other uses for the USB keys include Web access control, client token for Virtual Private Network access, replacement for password generator tokens and storage of credentials, certificates and licenses.

In a news release dated 19 January 1999, Rainbow Technologies, Inc. announce a new line of USB tokens for VPNs (virtual private networks) which provides end user client authentication to VPNs and enables operator access to secured network equipment. Features of these tokens include "Internet security small enough to fit on a key-ring" and "personalization for the end user". The tokens allow a user to keep personal information in his or her pocket rather than on a hard drive.

A new "unique per individual" model of its USB based tokens was announced by Rainbow Technologies Inc. on 15 March 1999.

The disclosures of all publications mentioned in the specification and of the publications cited therein are hereby incorporated by reference.

SUMMARY OF THE INVENTION

The present invention seeks to provide improved flexibly connectible apparatus and improved methods for using the same.

There is thus provided, in accordance with a preferred embodiment of the present invention, a user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method including storing information characterizing each mobile user on an FCCS plug to be borne by that mobile user and accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the information characterizing the mobile user to perform at least one computer operation.

Further in accordance with a preferred embodiment of the present invention, at least one computer operation comprises authentication.

Also provided, in accordance with another preferred embodiment of the present invention, is a an FCCS plug device to be borne by a mobile user, the FCCS plug device including a portable device which mates with a flexibly connectible computer system and comprises a memory and information characterizing the mobile user and stored in the memory accessibly to the flexibly connectible computer system.

Also provided, in accordance with another preferred embodiment of the present invention, is a population of FCCS plug devices to be borne by a corresponding population of mobile users, the population of FCCS plug devices including a multiplicity of portable devices each of which mates with a flexibly connectible computer system and comprises a memory and information characterizing each mobile user in the population of mobile users and stored, accessibly to the flexibly connectible computer system, in the memory of the FCCS plug device to be borne by the mobile user.

Additionally provided, in accordance with another preferred embodiment of the present invention, is an FCCS plug device including a mating element operative to mate with a flexibly connectible computer system and a memory connected adjacent the mating element, thereby to form a portable pocket-size plug, wherein the memory is accessible to the flexibly connectible computer system via the mating element.

Also provided, in accordance with another preferred embodiment of the present invention, is an FCCS plug device including a mating element operative to mate with a flexibly connectible computer system and a CPU connected adjacent the mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via the mating element.

Further in accordance with a preferred embodiment of the present invention, the FCCS plug device also comprises a CPU connected adjacent the mating element, thereby to form a portable pocket-size plug, wherein the CPU has a data connection to the flexibly connectible computer system via the mating element.

Still further in accordance with a preferred embodiment of the present invention, at least one computer operation comprises digital signature verification and/or controlling access to computer networks.

Further in accordance with a preferred embodiment of the present invention, the information characterizing each mobile user comprises sensitive information not stored in the computer system, thereby to enhance confidentiality.

Also provided, in accordance with another preferred embodiment of the present invention, is a user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method including

storing confidential information not stored by the flexibly connectible computer systems on an FCCS plug to be borne by an individual user within the population of mobile users and

accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the confidential information to perform at least one computer operation, thereby to enhance confidentiality.

Preferably the apparatus also includes a microprocessor operative to receive the USB communications from the USB interface, to perform computations thereupon and to provide results of the computations to the data storage unit for storage and/or for encryption and/or for authentication and/or for access control.

The term "USB port" refers to a port for connecting peripherals to a computer which is built according to a USB standard as described in USB specifications available over the Internet at www.usb.org.

The term "USB plug" or "USB key" or "USB token" refers to a hardware device whose circuitry interfaces with a USB port to perform various functions.

The term "smart card" refers to a typically plastic card in which is embedded a chip which interacts with a reader, thereby allowing a mobile bearer of the smart card to interact with a machine in which is installed a smart card reader, typically with any of a network of machines of this type.

Also provided in accordance with a preferred embodiment of the present invention is an electronic token, which preferably mates with a flexible connection providing

port such as the USB port of any computer system such as a PC, laptop, palmtop or peripheral. The electronic token preferably does not require any additional reading equipment. The token may authenticate information and/or store passwords or electronic certificates in a token which may be the size of a domestic house key.

Preferably, when the token is inserted into a flexible connection providing port, a highly secure "dual factor authentication" process (e.g. "what you have" plus "what you know") takes place in which (a) the electronic token is "read" by the host PCC or network and (b) the user types in his or her personal password for authorization.

Suitable applications for the electronic token include authentication for VPN, extranet and e-commerce.

The present invention also seeks to provide improved USB apparatus and improved methods for using the same.

There is thus provided, in accordance with another preferred embodiment of the present invention, USB key apparatus for interacting with a USB host via a USB port, the USB key apparatus including a portable device configured to fit the USB port, the portable device including a USB interface conveying USB communications to and from a USB host, a protocol translator operative to translate the USB communications from USB protocol, into smart card protocol such as an ISO7816 protocol, and from smart card protocol into USB protocol and a smart card chip operative to perform at least one smart card function such as authentication, encryption, access control and secure memory.

Also provided, in accordance with another preferred embodiment of the present invention, is USB key apparatus with data storage capabilities, the USB key apparatus including a portable device such as a PCB, configured to fit the USB port, the portable device including a USB interface conveying USB communications to and from a USB host and a data storage unit storing information derived from the USB communications.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1 which is a simplified block diagram of a flexibly connectible USB plug device including a CPU and a non-ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention.

A particular feature of the USB plug device of Fig. 1 is that it has data storage capabilities and is thus analogous to a memory smart card.

The USB plug device 10 comprises a PCB 25 which includes a microprocessor or CPU 30 such as a Motorola 6805, Cypress chip or Intel 8051; a USB interface device 40; firmware memory 50 serving the firmware of the microprocessor 30; RAM memory 60 of size sufficient to enable contemplated computations on the part of the microprocessor 30; and user data memory 70 which stores a user's data. Some or all of the USB interface device 40, firmware memory 50 and RAM memory 60 may be within the CPU 30.

The USB interface device 40 and/or the firmware memory 50 may be integrated inside the microprocessor 30.

The firmware memory may be any suitable type of memory such as but not limited to ROM, EPROM, EEPROM or FLASH.

The user data memory 70 typically does not include ISO7816-3 memory and may, for example, comprise any of the following types of memory: I^2C, XI^2C, 2/3 wire bus, FLASH.

As shown, the USB plug device 10 is configured to interact with any USB host 20 such as but not limited to a personal computer or Macintosh having a USB port. Key-host interaction is governed by a USB protocol such as the USB protocol described in the USB specifications available over the Internet at www.usb.org. USB packets pass between the USB host 20 and the USB interface chip 40. Each packet typically includes the following components:

a. USB header;

b. Data to be stored/read on the user's data memory 70, plus additional information required by protocols of the memory chip 70, such as but not limited to the address to store/read the data, the length of data to store/read, and CRC checksum information.

c. USB footer.

The flow of data typically comprises the following flow:

The USB interface chip 40 receives USB packets from the USB host 20, parses the data, and feeds the parsed data to the microprocessor 30. The microprocessor 30 writes the data to, or reads the data from, the firmware memory 50, the RAM 60 or the user's data memory 70, using each memory's protocol.

In read operation, the microprocessor 30 passes the data to the USB interface chip 40 which wraps the data in USB packet format and passes it to the host 20.

Fig. 2 is a simplified block diagram of a USB plug device, constructed and operative in accordance with a preferred embodiment of the present invention, which is a one-piece smart card reader and smart card chip preferably providing both secured storage and cryptographic capabilities. The USB plug device of Fig. 2 includes both a CPU and a smart card chip (ICC) memory 170, typically a ISO7816 (T = 0/1) protocol-based chip communicating with the CPU 130 using an ISO7816-3 protocol. The apparatus of Fig. 2 is similar to the apparatus of Fig. 1 except that no separate user's data memory 70 is provided. The size of the RAM 160 is typically at least 262 bytes in order to support the ISO 7816_3 T=0 or T=1 protocols.

Each packet typically includes the following components:

a. USB header;

b. ISO7816-3 T=0/1 protocol packet;

c. USB footer.

The flow of data in the apparatus of Fig. 2 typically comprises the following flow:

The USB interface chip 140 gets USB packets from the USB host 120. The USB interface chip 140 parses the data and passes it to the microprocessor 130. The data, which typically comprises a ISO7816-3 T=0/1 formatted packet, is passed by the microprocessor to the smart-card 170 in a ISO7816-3 protocol. The microprocessor 130 gets the response from the smart card 160 and passes the data to the USB interface chip 140. The USB interface chip 140 wraps the data in USB packet format and passes it to the host 120.

A particular advantage of the embodiment of Fig. 2 is that smart card functionality is provided but there is no need for a dedicated reader because the plug 110 is connected directly to a USB socket in the host 120.

The invention shown and described herein is particularly useful for computerized systems serving organizations which process sensitive information such as banks, insurance companies, accountants and other commercial organizations, and professional organizations such as medical or legal organizations.

Conventional computer systems include a computer (comprising a motherboard) and at least one peripherals. The computer has a number of different ports which respectively mate with the ports of the various peripherals. Each port typically can mate with only certain peripherals and not with other peripherals. For example, the keyboard cannot be connected to the computer via the computer's printer port.

In state of the art computer systems, also termed herein "flexibly connectible computer systems", the computer and the peripherals each include at least one identical ports having mating ports on any other computer and any other peripheral such that any peripheral can be selectably connected to any computer or to any other peripheral. Also, a peripheral may be connected to the computer not directly as in conventional systems but rather via another peripheral. There is generally always a port available on one or more connected peripherals in an existing computer system such that another peripheral can generally always be connected to an existing computer system.

One example of a flexibly connectable computer system is a USB (universal standard bus) system in which the computer and each peripheral includes a USB port. Another example of a flexibly connectable computer system is the recently contemplated Firewire system.

A "USB plug" is a portable device which mates with a USB system and, as opposed to peripherals which contain mechanical elements, typically comprises only memory and/or CPU and therefore is typically pocket-size. More generally, a USB plug is an example of a plug which can be plugged into a flexibly connectible computer system (FCCS).

The term "FCCS plug" is used herein to refer to a portable device which mates with a flexibly connectible computer system and, as opposed to peripherals which contain mechanical elements, typically comprises only memory and/or CPU and therefore is typically pocket-size. It is appreciated that because each peripheral connected onto a flexibly connectible computer system typically has at least one port, therefore, a flexibly connectible computer system of any configuration typically has at least one vacant port available to interact with an FCCS plug. USB tokens and Rainbow tokens are both examples of FCCS plugs.

Typically, each of the plurality of computer system units (computer and one or more peripherals) forming a computer system has at least two identical female sockets and these are interconnected by means of male-male cables. In this embodiment, the FCCS plug may comprise a male socket. However, it is appreciated that any suitable mating scheme may be employed to mate the computer system units and the the FCCS plug of the present

invention.

A known use for FCCS plugs is use in conjunction with software having plug-recognizing capability. Aladdin and Rainbow both market software which is operative only if the host computer system in which a particular software copy resides has plugged into it an FCCS plug which is recognized by the software copy. The Aladdin and Rainbow plugs are not used for authentication.

Computer systems are often used to receive information characterizing a mobile user, who is one of a population of mobile users, and to process this information. Such information may comprise user identity authentication information, banking information, access rights information, etc. Conventionally, this information is stored on a smart card which is borne by the user and is presented to the computer system by him. However this requires the computer system to be equipped with a smart card reader, a special piece of equipment dedicated to reading the smart card.

According to a preferred embodiment of the present invention, information characterizing a mobile user is stored on an FCCS plug. Particular advantages of this embodiment of the present invention is that the information is easily borne by the user, on a pocketsize substrate, that any flexibly connectible computer system of any configuration is typically capable of interacting with the user via the FCCS plug, and that no dedicated equipment is required by the computer in order to carry out the interaction.

Reference is now made to Fig. 3 which is an exploded front view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB key device of Fig. 1. As shown, the FCCS plug of Fig. 3 comprises a housing typically formed of two snap-together planar cover elements 200 and 210, between which reside a USB connector 220 and the PCB 25 of Fig. 1. The USB connector 220 may, for example comprise a USB PLUG SMT <ACN-0213> device marketed by Aska Technologies Inc., No. 15, Alley 22, Lane 266, Fu Teh, 1st Rd., Hsi Chih, Taipei Shien, Taiwan. The PCB 25 bears the elements 30, 40, 50, 60 and 70 of Fig. 1. Firmware managing the memory 240 may reside on the USB interface controller 230.

Reference is additionally made to Fig. 4 which is an exploded view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB key device of Fig. 2. As shown, the FCCS plug of Fig. 4 comprises a housing typically formed of two snap-together planar cover elements 200 and 210, between which reside the USB connector 220 and a PCB 125. The PCB 125 bears the elements 130, 140, 150, 160 and 170 of Fig. 2. Firmware managing the smart card

chip 250 may reside on the USB interface controller 230.

Smart card functionalities which are preferably provided by the FCCS plug of the present invention include:

1. Controlling access to computer networks: Smart card or plug has ID information, network authenticates and allows access on that basis. Authentication may be based upon "what you have", "what you are" e.g. biometric information and "what you know" (e.g. password).

2. Digital signatures or certificates for verifying or authenticating the identity of the sender of a document.

3. Storage of confidential information e.g. medical information. A smart card or plug may store confidential information and interact with a network which does not store the confidential information.

Figs. 5A - 5B pictorially illustrate a user-computer interaction method provided in accordance with a preferred embodiment of the present invention for use by a population of flexibly connectible computer systems 300 and a population of mobile users. Information characterizing each mobile user, e.g. name and ID, is loaded into the memory of an FCCS plug 310 to be borne by that mobile user, typically via a USB interface controller such as unit 230 of Fig. 3.

The plug can then be connected to one of the flexibly connectible computer systems and the information characterizing the mobile user employed to perform at least one computer operation typically comprising a conventional smart card functionality such as authentication.

Features of a preferred embodiment of the present invention are now described:

a. The need for enhanced user authentication

* Authentication is the basis for any information security system. The ability to authenticate local and remote users is a critical issue for any LAN/Intranet, multi-user environment

b. The need for encryption and confidentiality

* Content encryption & confidentiality becomes an important issue for both the corporation and the individual users

c. The need for password and Sign-On security

* Password security and user password management are key issues for network corporate users. Passwords represent the single most important security concern in any

computing environment

There is a need today for hardware-based PC security tokens

* Sign-On-Key (SOK) is a hardware-based token that seamlessly integrates with Operating Systems & Applications to provide:

- a user authentication key
- a basis for encryption system
- better Sign-On security and enhanced user password management
- Software Security

Authentication - 3 Basic Elements

* Something you know --> Password
* Something you have --> Sign-On-Key
* Something you are --> e.g., Bio-metrics

* Assumption: Two out of the above three provide "good-enough" security.

Encryption

* The need to encrypt data, files, disks and information flow is evident.
* An hardware-based token with cryptographic abilities can enhance security and ease-of use.

Sign-On - Where are Passwords used?

* Log on to your O/S
* Log on to your Network (Local, Remote)
* Log on to the Internet/ISP
* Log on to protected Web pages
* Log on to GroupWare/Communications applications
* Log on to other sensitive password-protected applications
* MS Office & other protected files
* PC Boot protection (Bios Password)

Sign-On - Major Security Risks

The Sign-On Process

The Sign-On-Key is a security hardware token, linked by the user to the required applications. Once installed the -Sign-On-Key becomes a part of the log-on process. Sign-On-Key provides the user with many security and other functional benefits.

What Can Sign-On-Key Do For a User?

* Sign-On Security

- Enhance security & authentication. The Sign-On-Key is required in addition to the user password

* Sign-On Simplicity

- Simplify log-on process and eliminate the need for a password. The Sign-On-Key replaces the password

* Password Automatic Re-verification

- Check for Sign-On-Key periodically

* Single-Sign-On

- One Sign-On-Key replaces several passwords for several applications

* Mobility & Remote Computing

- Sign-On-Key identifies remote users

- Sign-On-Key can be used as a data secure container

- Theft deterrent of mobile PCs

* General Purpose Security Token

- File & data Encryption

- Authentication

- Certificate Key Holder

Sign-On-Key Various Options

* Several hardware devices may operate as Sign-On-Keys:

- Sign-On-Key USB - A small key that connects to the new standard USB port. USB ports are becoming the new connectivity standard for PCs and Macintosh

- Sign-On-Key SC - A smart card based Sign-On-Key. Can be used with any standard smart card drive

Sign-On-Key USPs & Advantages

* Simple, intuitive, easy to use, attractive token

* The key IS the token IS the connector

* Low cost

* High security

* High functionality
- Memory inside token
- Processing power
- Automatic Password Re-verification
- Multi token connectivity
* The Agents' solution

Sign-On-Key Architecture

Full Blown System.

Sign On Agents

* The Sign-On-Agent is a software interface between the Sign-On-Key and the application.
* The Sign-On-Boot is a special interface for the PC boot password.
* Agents may be provided for:
- OS/NetWare - e.g., Windows NT, 95/98, 3x, Novell, Unix
- GroupWare/Mail - e.g, Lotus Notes, Outlook, Eudora,
- Enterprise Applications - e.g., SAP, Baan, MK, Oracle, Magic
- Web Browsers - e.g., Explorer, Navigator

The Most Trivial Agent - Windows NT

* The most trivial Agent will replace the Windows Login session
* By doing so Users may gain
- Windows Login Extra security
- Windows Login simplification (Sign-On-Key replaces password)

Sign-On-Key Web Browsers' Agent/System

* Sign-On-Key can be used as an authentication token to monitor access to secured web pages
* Web content providers need to authenticate, manage and provide access to their customers

Sign-On-Key API (SDK)

* Sign-On-Key API is the interface level between the Sign-On-Key and 3rd parties' applications.
* This API may be published and opened for usage by certification providers, security companies and SSO companies.
* The Sign-On-Key API will also provide encryption & protected memory storage services
* Sign-On-Key API may be PKCS #11 based/compatible

The Sign-On Process (No CA)

* Installation

- User installs Agents for required applications

- User defines Sign-On Parameters for each application

- User stores Sign-On information in Sign-On-Key

* Sign-On

- Application is started

- Application reaches its Sign-On dialog

- Application communicates with the Sign-On-Key

- Sign-On permission is granted based on Sign-On-Key

Sign-On-Key As a Secure Container

* In addition to unique Key ID, Sign-On-Key will contain personal protected memory area

* This memory area can be used for storing sensitive information and Certificates

* Applications' ID keys like Lotus Notes ID file or PGP keys can be stored in this memory

* Doing so - Sign-On-Key can be used to increase mobile computing security. Files IDs are stored in Sign-On-Key instead of disk

Sign-On-Key An Encryption Engine & Sign-On-Key Crypt

* Sign-On-Key can be used as an encrypting device

* An encryption API may be provided, e.g., a 100% smart card compatible Sign-On-Key implementation

* Sign-On-Key Crypt is a Data/File/Hard disk encryption utility based on Sign-On-Key.

Sign-On-Key Certification Toolkit

* SOK may use PKCS #11 and X509 and store certificates and/or digital IDs.

Sign-On-Key comprises:

* Sign-On-Key USB Token

* HASP

* Hardlock

* Initial Sign-On-Key functionality (Unique ID, personal protected memory)

* Sign-On-Key USB extension cable

* Sign-On-Key Smart Card Token

* Sign-On-Key API (PKCS #11 compliant)

* Entrust compatibility/link

* Windows NT Agent

* Navigator and/or Explorer Agent (S/Mime)
* Key Plus Crypt (Beta release)
* Secure Screen Saver
* Initial marketing package

* USB proliferation & Windows 98/NT availability are key issues
* In the US, Germany & Israel all new PCs shipped are USB equipped.
* Section in Early Development stage.
* Security Dynamics, ActivCard & Vasco control the market with 1st generation time-based, one-time password or challenge-based tokens
* security vendors will look to expand their market share with second generation integrated smart card offerings which will support cryptography, digital signature storage and processing activity

USB: The Better Connection
* Almost unlimited port expansion
* No add-in cards for new peripherals
- no setting of IRQs, DMAs, etc.
* One connection type (plug and port)
- variety of peripherals
- no more guesswork
- simple setup, just plug in and go
USB: The Better Connection
* Addresses need for speed, multimedia
- 12 Mb/s, Asynch (bulk) & Isoch (real time) data
- stereo-quality digital audio
- high frame-rate video (with compression)
- high latency applications (force-feedback)
* No power bricks with many new peripherals
- USB supplies up to 500mA
* PC User experience is vastly improved
- Fewer returns and increased sales potential

It is appreciated that USB is only one example of a flexible connectivity

standard and the present invention is not intended to be limited to USB.

It is appreciated that the software components of the present invention may, if desired, be implemented in ROM (read-only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention is defined only by the claims that follow:

4. Brief Description of Drawings

Fig. 1 is a simplified block diagram of a USB plug device including a CPU and a non-ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 2 is a simplified block diagram of a USB plug device including a CPU and a ISO7816 memory, the USB device being constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 3 is an exploded front view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB plug device of Fig. 1;

Fig. 4 is an exploded view of an FCCS plug constructed and operative in accordance with a preferred embodiment of the present invention and implementing the USB plug device of Fig. 2; and

Figs. 5A - 5B pictorially illustrate a user-computer interaction method provided in accordance with a preferred embodiment of the present invention for use by a population of flexibly connectible computer systems and a population of mobile users.

FIG. 1

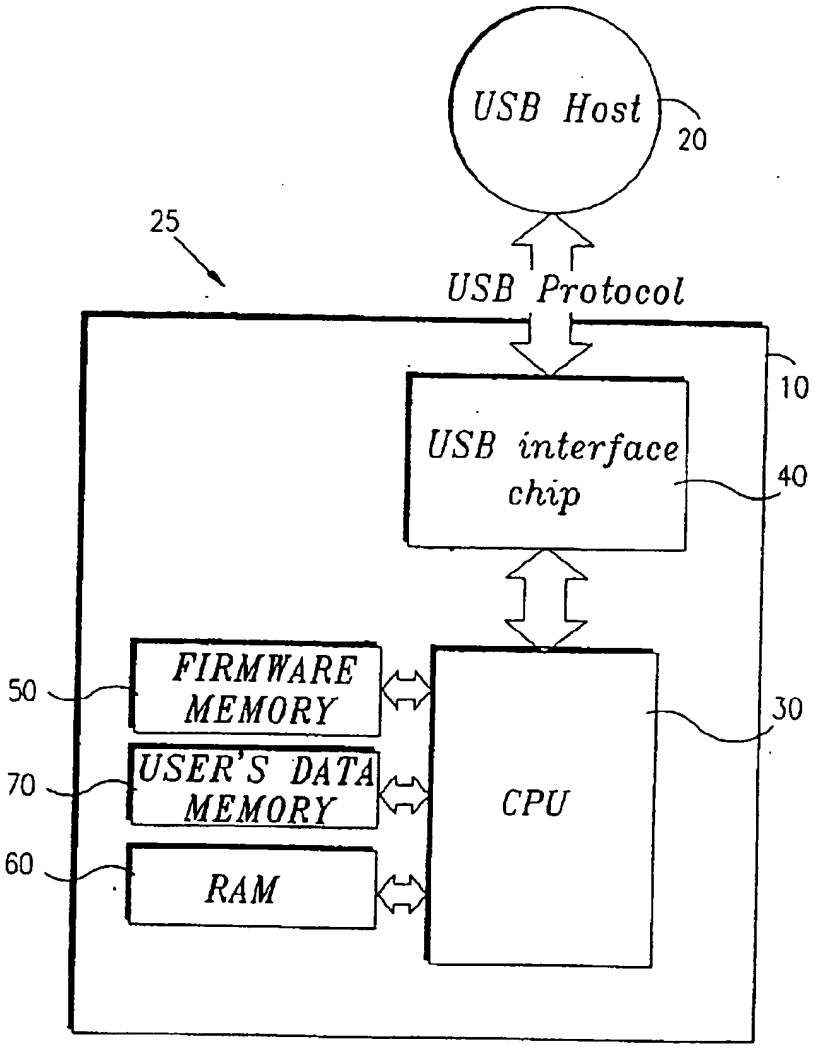

USB Host
20
25
USB Protocol
10
USB interface chip
40
FIRMWARE MEMORY
50
USER'S DATA MEMORY
70
RAM
60
CPU
30

FIG. 2

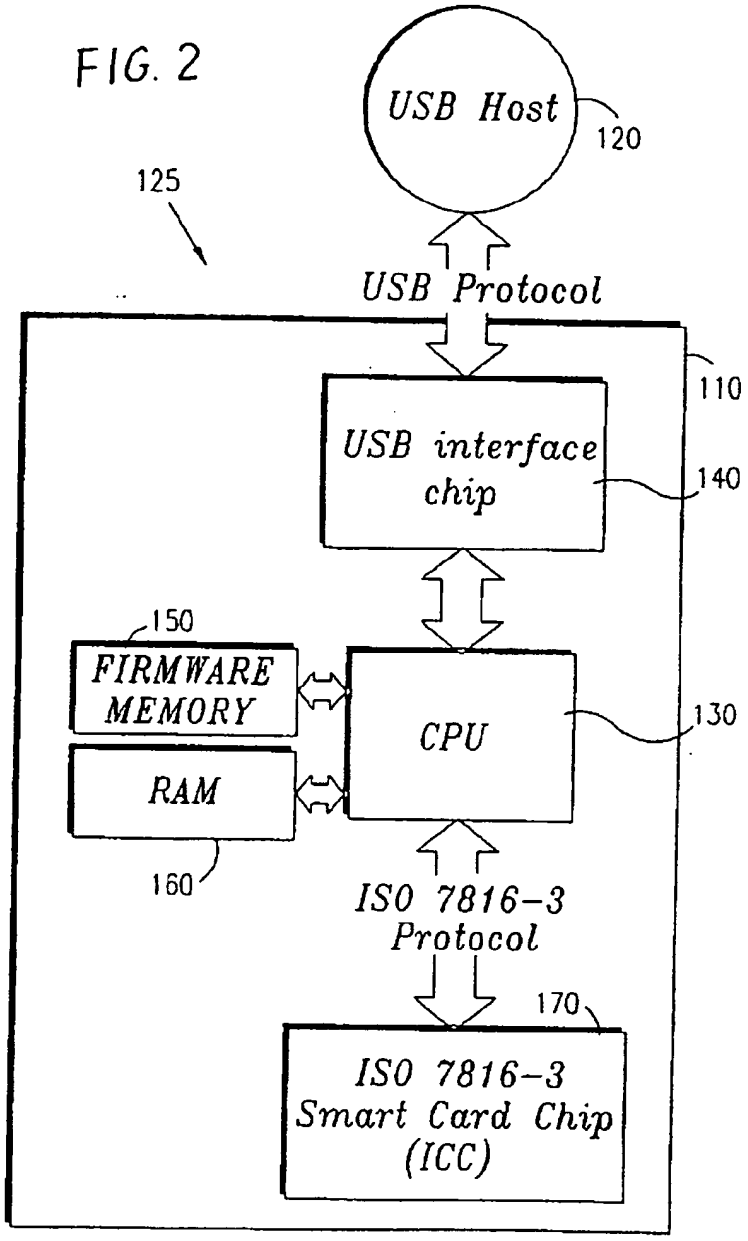

USB Host
120
125
USB Protocol
110
USB interface chip
140
150
FIRMWARE MEMORY
CPU
130
RAM
160
ISO 7816-3 Protocol
170
ISO 7816-3 Smart Card Chip (ICC)

FIG. 3

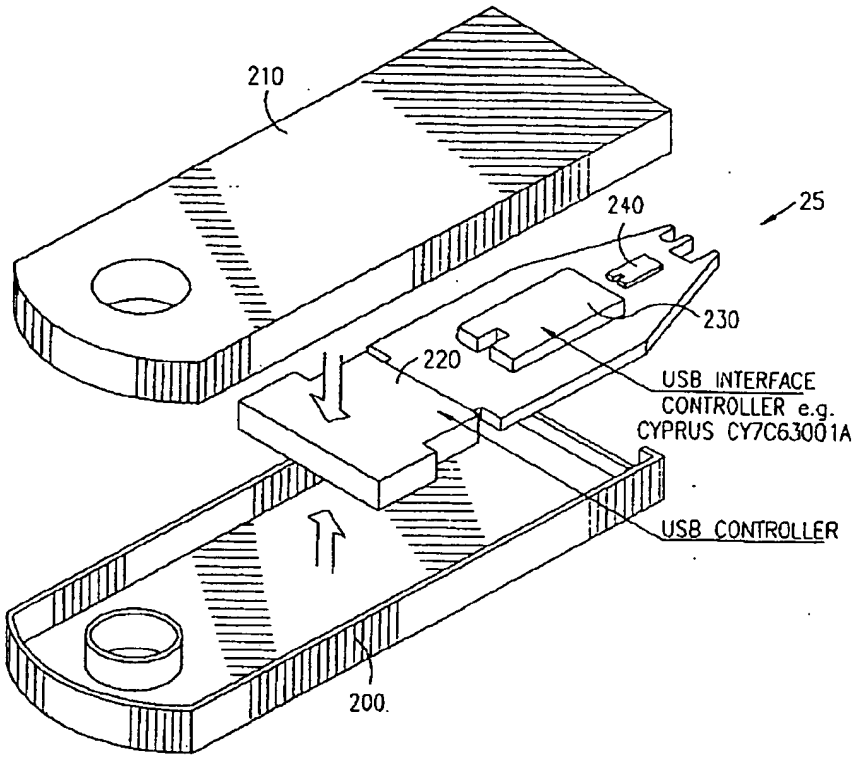

210
240
25
230
220
USB INTERFACE
CONTROLLER e.g.
CYPRUS CY7C63001A
USB CONTROLLER
200

FIG. 4

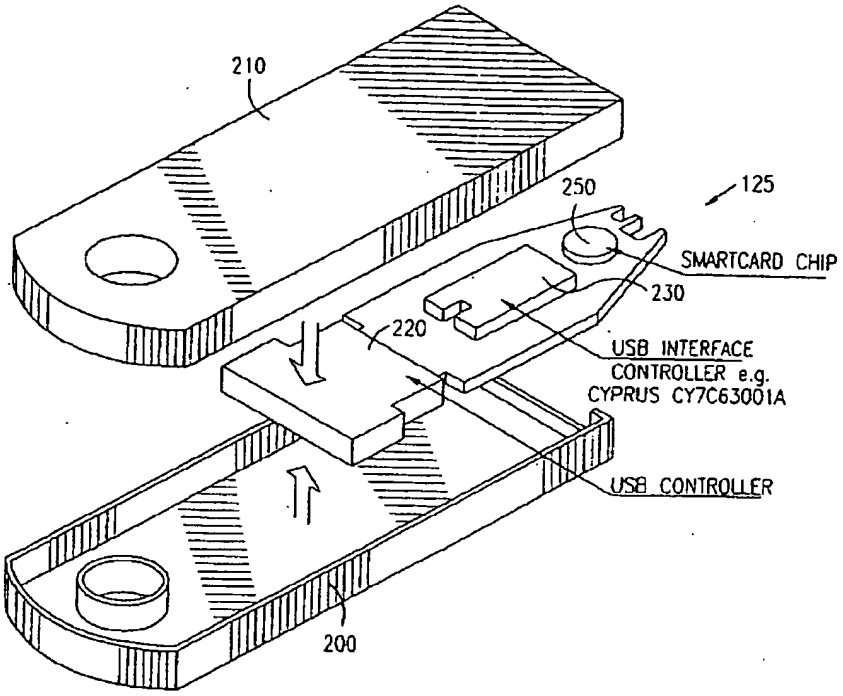

210
250
125
SMARTCARD CHIP
230
220
USB INTERFACE
CONTROLLER e.g.
CYPRUS CY7C63001A
USB CONTROLLER
200

FIG. 5B

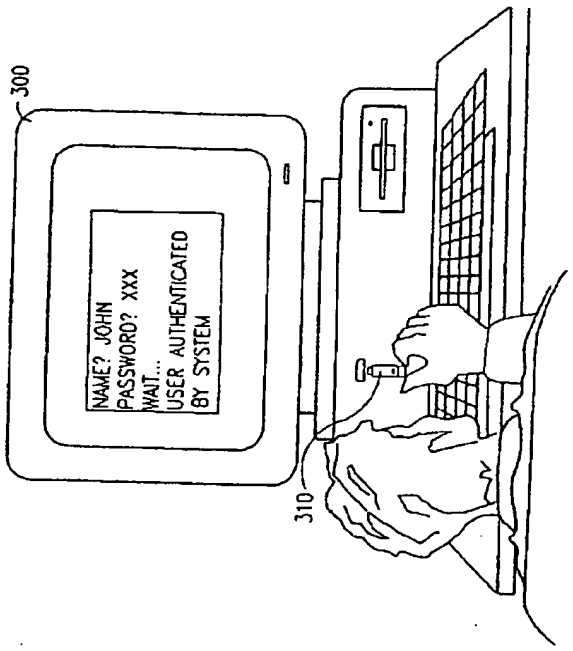
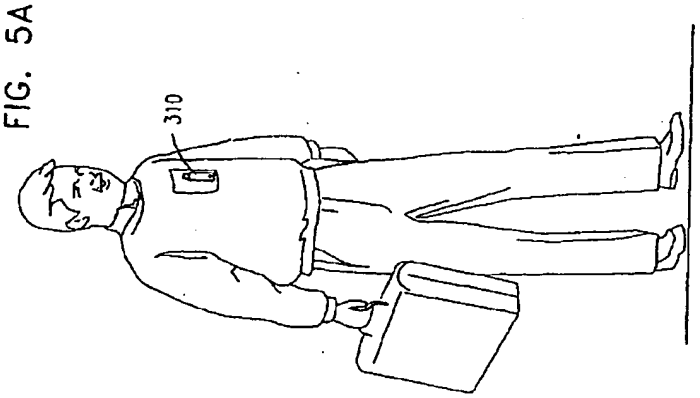


FIG. 5A



1. Abstract

A user-computer interaction method for use by a population of flexibly connectible computer systems and a population of mobile users, the method comprising storing information characterizing each mobile user on an FCCS plug to be borne by that mobile user; and accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the information characterizing the mobile user to perform at least one computer operation.

2 Representative Drawing

Fig. 1

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.